Security Testing Report

IGT Solutions

CAD GHS 1.0.1

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Table of Contents

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Document Version Control

Name of the document : CAD GHS 1.0.1 Security Testing Report		
Version: 6.0	**Intake ID:**	**2695**
Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	**Document ID:**	**PRHC/C40/SVN/80639**
Author: Sai Praneetha Bhaskaruni, Harshal Kukade	**Effective Date:**	**27 July 2023**
Reviewed by: Chaitra N Shivayogimath		

Document History

Version	Date	Author	Section	Changes
0.1	16 Dec 2022	Chaitra N Shivayogimath	Complete	Initial Draft
1.0	19 Dec 2022	Ashwin K K	Complete	Final Review
1.1	10 Feb 2023	Chaitra N Shivayogimath	Complete	Retest and Reporting
2.0	13 Feb 2023	Ashwin K K	Complete	Final Review
2.1	19 April 2023	Chaitra N Shivayogimath & Meba Meria Jacob	Complete	Initial Draft
3.0	19 April 2023	Shabana Bagum	Complete	Final Review
3.1	27 April 2023	Meba Meria Jacob	Complete	Revalidation of 7.3, 7.5, 7.8 & 7.10

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

4.0	**27 April 2023**	**Chaitra N Shivayogimath**	**Complete**	**Final Review**
4.1	**02 May 2023**	**Meba Meria Jacob**	**Complete**	**Revalidation of 7.3 & 7.8**
5.0	**02 May 2023**	**Chaitra N Shivayogimath**	**Complete**	**Final Review**
5.1	**05 May 2023**	**Meba Meria Jacob**	**Complete**	**Revalidation of 7.4 &7.5**
5.2	**05 May 2023**	**Chaitra N Shivayogimath**	**Complete**	**Final Review**
5.3	**24 July 2023**	**Harshal Kukade,** **Sai Praneetha Bhaskaruni**	**Complete**	**Addition & Review**
6.0	**27 July 2023**	**Chaitra N Shivayogimath**	**Complete**	**Final Review**

Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	SakethM.Jain@philips.com; Chandrashekar.Natarajan@philips.com; Priya.Vijayachandran@philips.com; anand.kumarjaiswal@philips.com sreenath.kooloth@philips.com karthik.srinivasan@philips.com

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting
CORS	Cross Origin Resource Sharing
CAD	Coronary Artery Disease
NBX	New Business Creation
B2B	Business To Business
B2C	Business to Consumer
GHS	Guided Health Services

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below	
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located here. Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Categories for vulnerability classification	
Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten – 2014

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

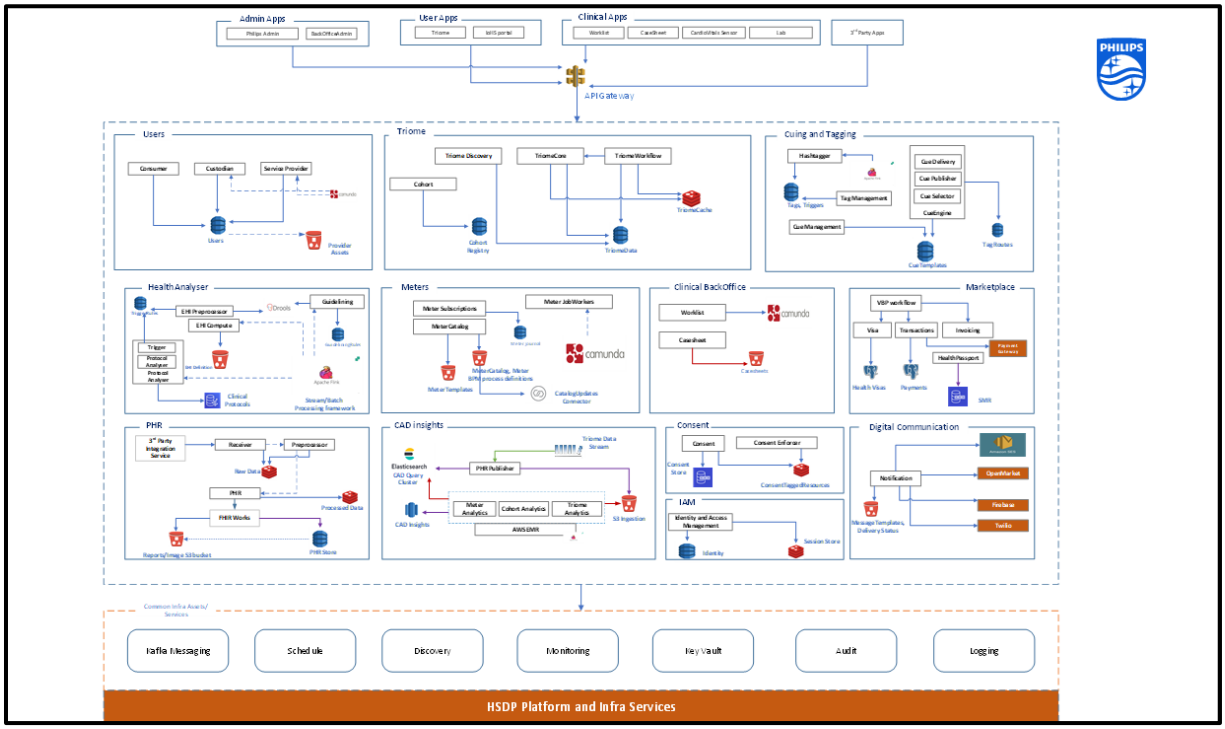
2. System Details & Architecture

A Conceptual Overview of CAD GHS Web application:

- Engages consumers towards their cardiac health through monitoring, forecasting and guide-lining
- A proactive health services marketplace (B2C and B2B) backed by outcome-based services (meters)
- Post MVP, expand the solution to assurance services for large cohorts based on protocol-based clinical guidance and AI-driven differential diagnosis

Test Environment: Validation

Architecture Diagram:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

3. Scope

The scope of this security assessment is to perform ***Grey-Box*** security testing to find security threats that may come from a malicious outsider or insider user of the **CAD GHS 1.0.1.** Security testing on **Web application/Web Services** of the **CAD GHS 1.0.1** is performed.

The following list includes some examples of major activities performed during the assessment:

Web Application/Web Services:

1. Retest of previous **Web** findings & fixes:
    - Missing Security Headers.
    - Server Banner Disclosure.
    - OTP Rate Limit (IAM) - login page redirection.
    - Reuse of old OTP within 4minutes.
2. Fresh test of 2 New **Web Services/API** Endpoints: View Report Feature
    1. GET: <BaseURL>/engagement/report
    - Params
        - reportStartDate=2023-07-12T17:17:51Z
        - reportEndDate=2023-07-13T11:02:49Z
        - reportType=BEATS
        - userId=<UUID>
    2. POST: <BaseURL>/engagement/report
    - Payload

```
{
  "assessmentRecordIds": [

  ],
  "userId": "",
  "requestId": "",
  "reportStartDate": "",
  "reportEndDate": ""
}
```

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

Follow "Test case execution" section to get the detailed about test cases.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

The test scope for this release is explained in the below table:

Start Date	End Date	Applications/Devices/IP's/URL's
19-July-2023	24-July-2023	CAD GHS: Web Application: • URLs: https://cad-consumer-app-int.us-east.philips-healthsuite.com/ • Environment: Test • Version: 1.0.1 • User Role: Consumer, Custodian, Admin Web Services: • URL: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report • Environment: Test • Version: 1.0.1 • User Role: Consumer, Custodian, Admin

CAD GHS is a web application which can be accessed via Mobile Web Browser.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Not in Scope

Below mentioned items are out of scope for the current security assessment:

- Source Code Review
- Network Testing
- AI Component
- Complete Web Application Testing (There are few features not developed yet)

Note: The environment provided was not stable. We have covered the testing of **CAD GHS 1.0.1** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

4. Executive Summary

Security Center of Excellence team engaged in activity to conduct security assessment of **CAD GHS 1.0.1** which included **Web Application/Web Service Testing** in scope. The purpose of the engagement was to evaluate the security of the **CAD GHS 1.0.1** against industry best practice criteria.

Note: Application is in nascent stage and features were not stable during testing phase.

Revalidation of previous findings carried out on 24th July, 2023 and updated the report accordingly. Identified 2 new vulnerabilities.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment of the product, security issues in the below area is found:

- Weak TLS/SSL Configuration
- Improper Session Management
- Sensitive Information in URL
- HTTPS Fallback Allowed
- Improper Error Handling
- Missing Security Headers
- Sensitive file exposed
- User Email Enumeration

During the security assessment of the product, security issues in the below areas were not found:

- CSRF Attacks
- Input Validation

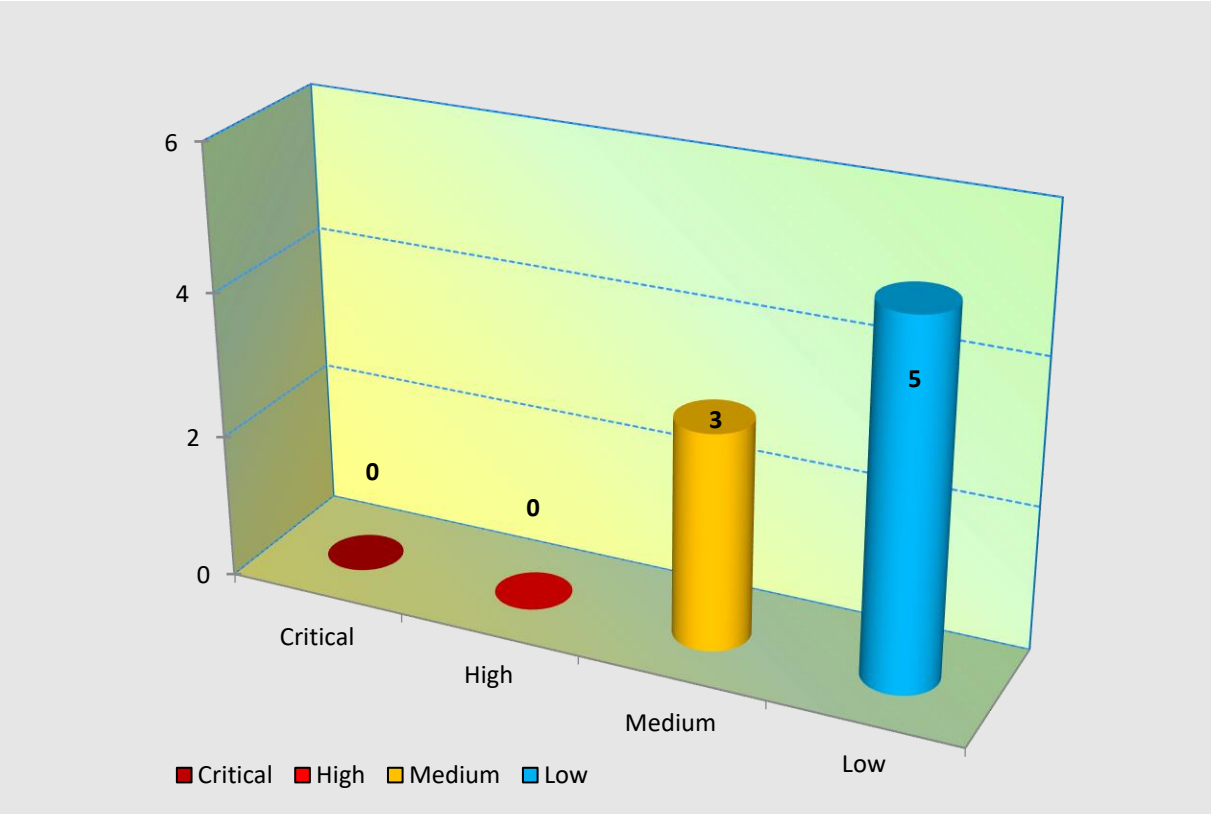
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

Note: The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.



Note: - 1 informational finding not included in Chart

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

5. Vulnerability Summary

The Findings and vulnerabilities from the assessment are tabulated below

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status (02 May 2023)	Revalidation Status (05/May/2023)	Revalidation Status (24/July/2023)
86078	Account Takeover: Privilege Escalation	High	Webapp/ WebService	NA	Closed	Closed	Closed
82881	Functionality Misuse Due to Missing Authentication	Medium	Webapp	NA	Closed	Closed	Closed
82752	Modifiable Redirect URI Parameter	Medium	Webapp	NA	Closed	Closed	Closed
82899	Rate Limiting Not Implemented	Medium	Webapp	NA	Open	Closed	Closed
82900	Client Side Validation Bypass	Informational	Webapp	NA	Open	Open	Closed
84070	Weak TLS/SSL Configuration	Medium	Webapp	NA	Open	Open	Open
85889	Improper Session Management	Medium	Webapp/ WebService	NA	Open	Open	Open
86079	Lack of Authorization	Medium	Webapp	NA	Closed	Closed	Closed
85892	Sensitive Information in URL	Low	Webapp/ WebService	NA	Open	Open	Open

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

82753	Misconfigured CORS	Low	Webapp	NA	Closed	Closed	Closed
82916	HTTPS Fallback Allowed	Low	Webapp/ WebService	NA	Open	Open	Open
82886	Server Banner Disclosure	Low	Webapp/ WebService	NA	Open	Open	Closed
85890	Improper Error Handling	Low	Webapp/ WebService	NA	Open	Open	Open
86080	Missing Security Headers	Low	Webapp	NA	Open	Open	Open
87720	Sensitive file exposed	Medium	Webapp	NA	NA	NA	Open
87721	User Email Enumeration	Low	Webapp	NA	NA	NA	Open
87725	Misconfigured CORS	Low	WebServices	NA	NA	NA	Closed

*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

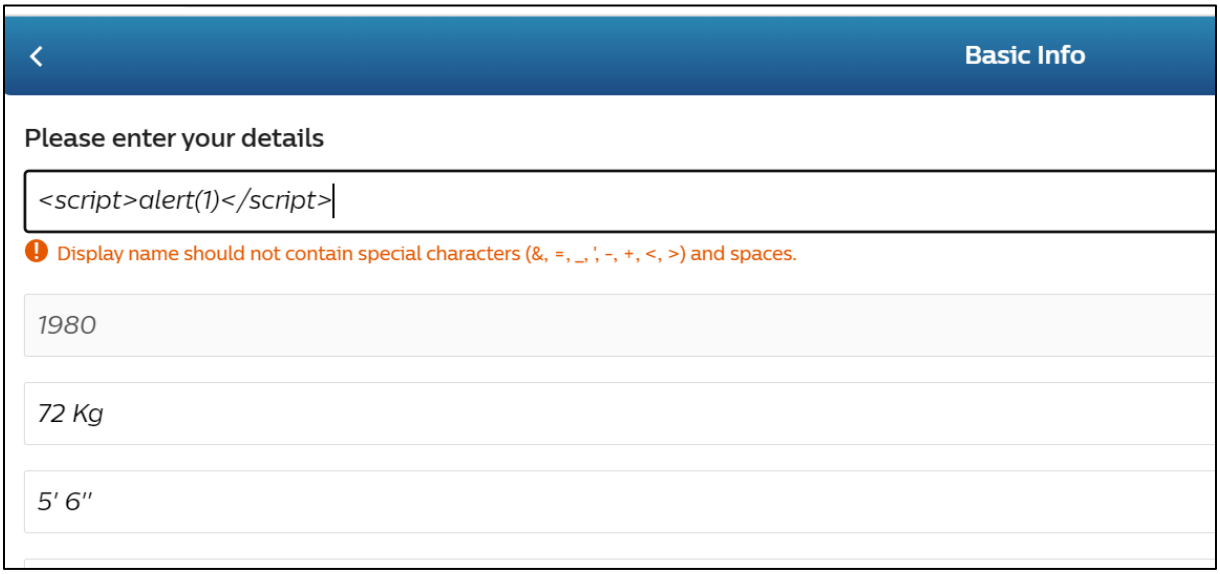
Printed copies are uncontrolled unless authenticated.

6. Observations

Below mentioned observations are not considered as Vulnerability but informative to the business.

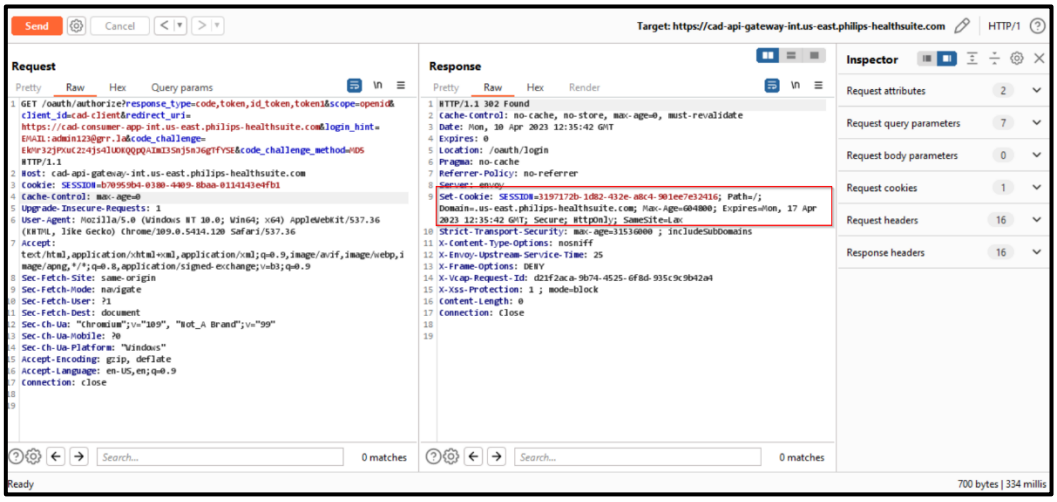
Observations which shows good implementation or best practice identified:

1. SCoE observed that strong input validation was in place for the user input.



Observations which shows weak implementation are:

1. It is observed that the oauth session cookie has certain misconfigurations: It is recommended to not scope the cookie to parent domain and secure flag should be set to the cookie.
    - Cookie is scoped to parent domain
    - Cookie expires after 1 week, which is very long duration.

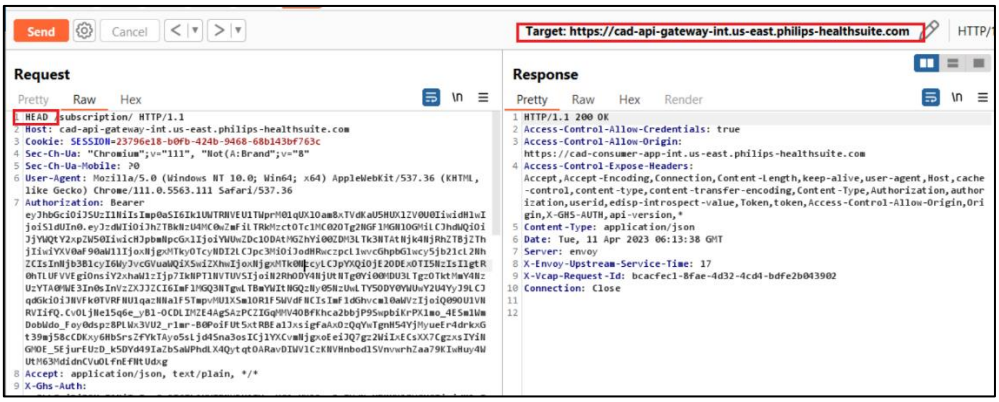


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

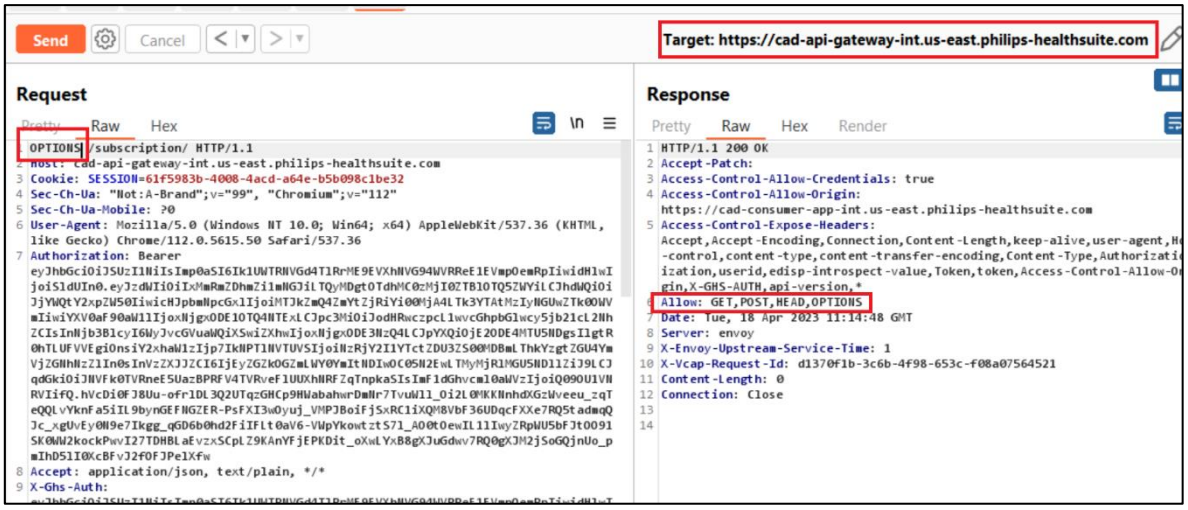
Printed copies are uncontrolled unless authenticated.

2. It was observed that the application does not properly invalidate a user's session on the server after the user initiates logout. User sessions remain active on the server, and any requests submitted including the user's session identifier will execute successfully, as though the user had made those requests. However, since the JWT token expires only after 20 min, the issue is kept in the observation.
   Refer Video POC

3. It is observed that for some API endpoints, HTTP methods are not properly defined.



HEAD Method allowed



HTTP/s supported methods shown in server response

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7. Detailed Vulnerability Report

7.1 Webapp/WebServices: Account Takeover: Privilege Escalation

Vulnerability Title	Account Takeover: Privilege Escalation
Vulnerability Category	A1 Broken Access Control
Severity	**High**
CVSS V3 Calculation	CVSS Base Score: 8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Description	**Vulnerability Description:** During the security assessment it was observed that a custodian user will be able to login as an admin user by just changing the login_hint:EMAIL: (or even PHONENUMBER) parameter after providing the OTP of that user. **Retest as of 18-Apr-2023:** The issue is fixed. **Retest as of 24-July-2023:** The issue is fixed. **Exploitability Rational:** An attacker needs to know the admin username(emailID) and be any valid user for the application. **Impact Rational:** Complete account takeover of the admin user can be done.
Affected Systems/IP Address/URL	https://cad-consumer-app-int.us-east.philips-healthsuite.com/signin WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report
Recommendation	It is recommended to validate the Email parameter in the /oauth/authorize? LoginHint parameter. This parameter should not be passed as a part of the GET request and it needs to be mapped to the code verifier/code challenge/session id.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Status	Closed

Supportive Evidence:

Please refer the video POC:

AccountTakeover.wmv

Retest Evidence as of 18 Apr 2023:

https://docs.philips.com/:v:/g/personal/chaitran_shivayogimath_philips_com/EScEBADh32NEocbA2RAUSXABKRfrqvORwvx16OveKDNCZQ?e=WJdBiH

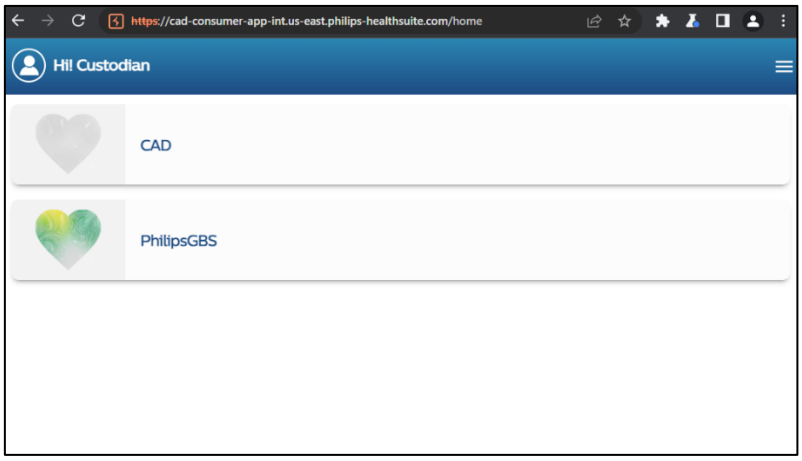
S_Acco untTakeover_2.wmv

Retest Evidence as of 24 July 2023:

Case 1: WebApp

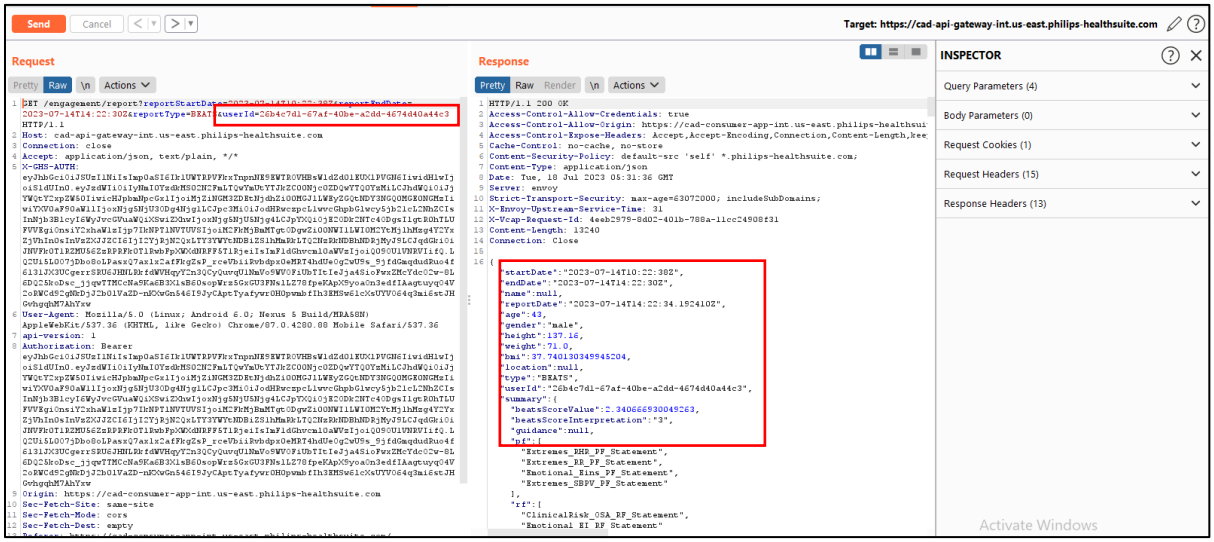
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



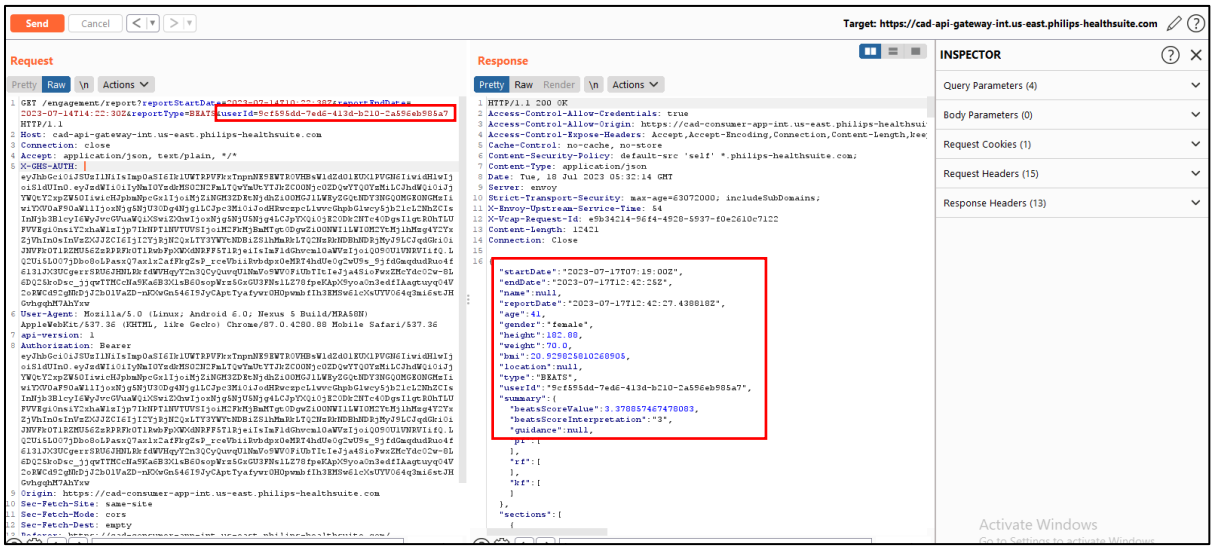
Test Evidence as of 24 July 2023:

Case 2: WebServices



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

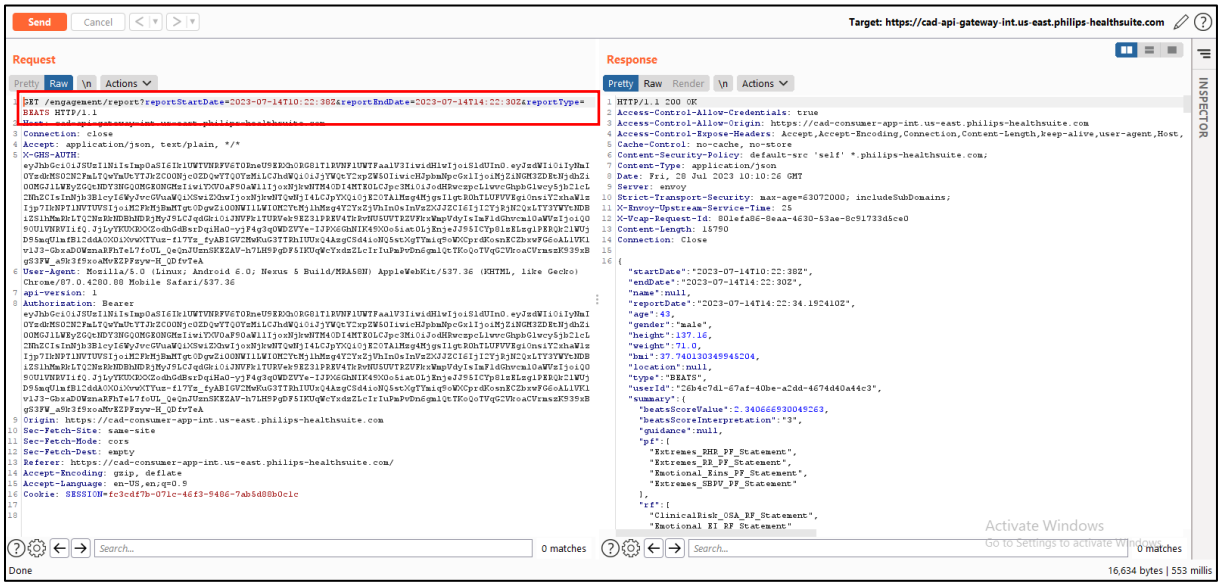
Printed copies are uncontrolled unless authenticated.



By replacing A's user id with B's user id, we are able to see the B's data.

Case 2:

Retest Evidence as of 28 July 2023:



User id is not visible. Not able to modify the same. Issue is fixed

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.2 Webapp: Functionality Misuse Due to Missing Authentication

Vulnerability Title	Functionality Misuse Due to Missing Authentication
Vulnerability Category	A7 Identification and Authentication Failures
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.9 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N
Description	**Vulnerability Description:** Upon Subscribing when we start Day 1, We get a URL to scan the Vitals of the patient. This URL can be accessed without any authentication and the vitals can be scanned. Upon clicking on save we are redirected to Login page. When we check for resume scan in the logged in Session the results would have already been submitted and we get to questionnaires part. We have observed that there is no JWT passed for this request. **Retest Status:** The issue is not fixed. The severity is reduced to Medium as the id and code in the URL expires in 5 mins. **Retest Status(17/April/2023):** Proper Authentication has been implemented. Hence the issue is CLOSED. **Retest as of 24-July-2023:** The issue is fixed. **Exploitability Rational:** Anyone having access to the scan URL can exploit this vulnerability. **Impact Rational:** Anyone can scan and use the application functionality even without authentictaion. The scan results gets saved even without authentication.
Affected Systems/IP Address/URL	https://cad-cardiovital-app-int.us-east.philips-healthsuite.com/?id=U2FsdGVkX1+zIu8S3Cgkt4iZIpUrn42ACWZz4usKlVKVFAAs/3WiD2e6O74a/YlzI9beNilENs4oShjRVU0ymc6mvpRah8FA7QglOTDetKfIjxxlXlMUbR88pxx71pQ7pivMPD1H4dXFQl8ij/mNJ1cr6R+pCrKxIx5+fDobJoHNe93xjb9Qup9QMWEmQabGJ6wVDI4etgtnrQsfKOMzaNKEj20KUzN9vjVp+HbM4qDusTVsJFhVqV9WECKcL2wJnDrqoSSxohlP2E1qNWudIFjbH6DED4szrj8p6J6gVkbfYYys7+yKnUaimpbpzz3Y0bbwVZRkUYeSOMwvleFg419vwkNLXCZIDLZyMzTnt5VxEw8DQGnFzwmcZn283x0qbAAJNmVphRkTd/8gPtnyvTm9AmkKueQGTfQPCqqIG72gi

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	KW3zKrzsSj/aKroUIUB6EeJaVsFum0/tNxTMjxwMdEAhfsctqUWzwXBm1hRQ+iElSnqWjxzGkBK5EASf5XFw5ApZ70G/5esQ8Yx4YtzTIHs5h8p1Z3eg8MEeaqL5oNnPw3PHlmqSRy71s0iSOHk+ZDvUV01XLj6T159qzX9pzrXgJ0a/OvbWJHZmbserIX+7EjuLQFca9NWX6PIESLQyoiIZu/D/Ge/tgRPTYZXYHWF5JENMIwLLlig9eTrSUqNdtAZ8z4jE6rbGEPgl0TTsruQTJ81fsAgK1+WgycGXCbhmwaLCsgB1YBWknhhmz8aoxktmkhW1vE+0w0JvbBvd4HXA54vQ2Mpi9FLAanKH4zWwrEumYrivQ0ZiPqyk/VhXB+dUY7faCZ5exsEHlvg8B5tSwVgcmKOWEDVBDhe37K+JO27seid03V1RTjjMBg2HtU81OehGIKimSj0YYxc7i1AibrwDifx6H7cSdUY8p+/XvcO2+qwll8ZvmnzVLkSNl3G0l/9u83JYpZeoZ4l35W0aEJLqCcLCSyJvHWKwWOWTCAj2d+32TeBQlbSZ8mrYpXAe3uRR8Jntvmi0nT0ClF2gEsP9AEZ96WTnFk3AB37FxlqVh5nSEFyxaEJGPD5QR0m116RKLjep0ZGGe4uEqvwfVESRZzCXEoSfPJ5gMMeRLZFmrMewT8ONCIwyVI0QhiEHjLRvNd1ek9udOH44cOMwlIsPMRmmfyI2QuYJJG/9Vtk/aeN5SKZzu6HfKbWvB2o7GeLnuT2rj6mz3IwIqz8HDvTRYq/jNvbF37V4+/WfhzpntC/XBB0nT4cftqVx0UPvNp26XFd/wsLa4IskCUW7UOMNYQ7lTNiSzzYm1D8cENVy2h59muROk1hfb4mlQkej9Jp8oK/HnZrh9zXghBdJDz6mLHlbFxuWeMmd5HoiNAa5gxO+sOGzdKYhHu7M/yPZOhl3jWulngZpKLjPdhJZ2XIoKL2CVXrwhh4WqtDfadEZIFpCO3KEVki1RIFoMLrxbWAo6zfh9GBib9WkXiK+m5CiE2jQvXLyJWFd+PZSxPBe5is0GLEVaQTo0GO/MEP1Xq8zreaSgmEyQUrCniN/RPwvc3fl7amclNLBJBN+2/bLcfdbz5NEplUu3BUhiF2lCgThYCIq1FM5Wqu2yQxo5lgJlcUtzm3gpg6yAbNAcSKM7R/Fvfghi1mvEM/1IyEnrgozBXAU2n+Oill34dqlMFZXzULkjr7tedAYd+7E5o8h/eZHRDwumRcWjEgbTROdWqi5Jx7KV+ubrNcEU9c9YhwrISeIlj7wa3Z80Fqs3MyygfSprC7FFnXP7A7E1YhMyL7IVA8SmiujtAFALT/B4fWyUD7JL+Radr/7tCYmhne5TE3AyI030dwkqU4MXPf+askXe3CcTzhLnxGdwUw89GdQFVVJxevbrJ8YADUNohAhJp4kczm1AWHsF7ugME5iHRxXJ3QoSFzRFutSq1SdY9D5RDUZVBWfTXDoZTN1us9WJTxxEovnmkARTHbOpgZ/11gTnhZ5ExQSb6GgGJ793msowwmiPCiLtk4mLn2MB7KVIloycxfL0gA428BF53cw9JOqyVThqoayHO9J3Rup2A0ADq0p925JSHNt+EX2DLdliacZGZJ9KC0j9sW2XyMDMbJ1thxk3+tgT6B5c+Xy0aCOcRs7Eq8Fq9ilANfynLis2mBNzT583LzKXGdfOGfk0IQCT8jQdyMU+kL https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=8545169a917ede5f8b84bf03b1ef3be556a2b6917c824c6346&login_hint=9916337921
Recommendation	Authentication should be enforced for all resources that require any form of restriction from users. There should be session handled for this feature
Status	**Closed**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

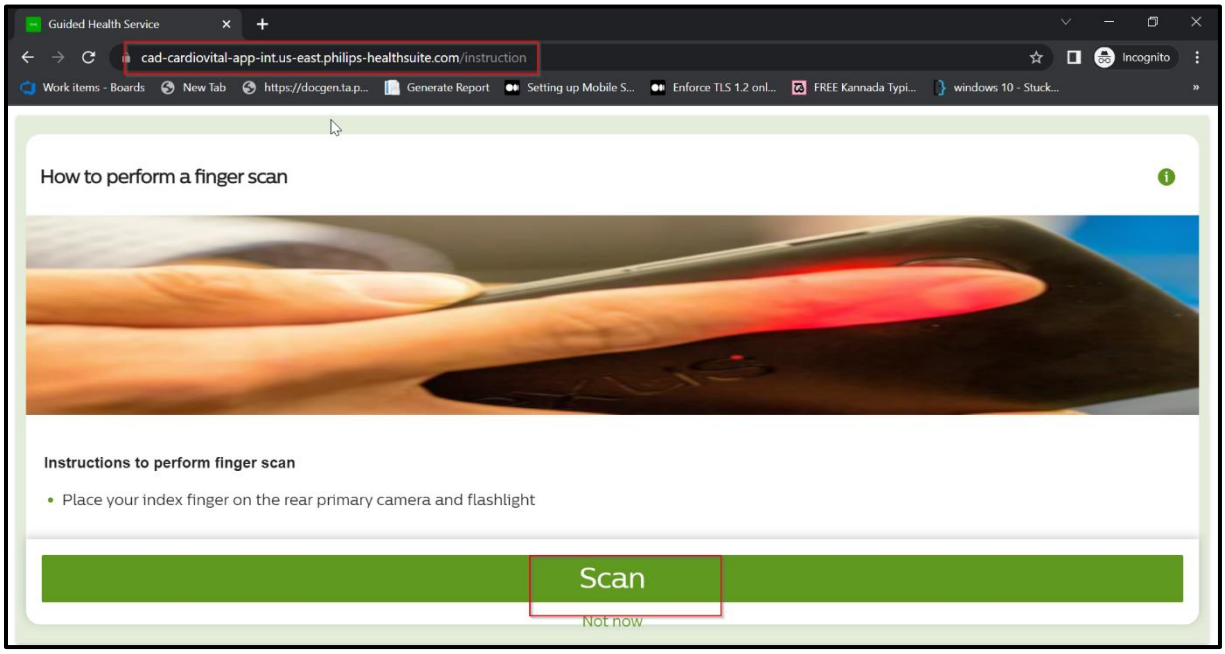
Steps to Reproduce

Refer the video POC:

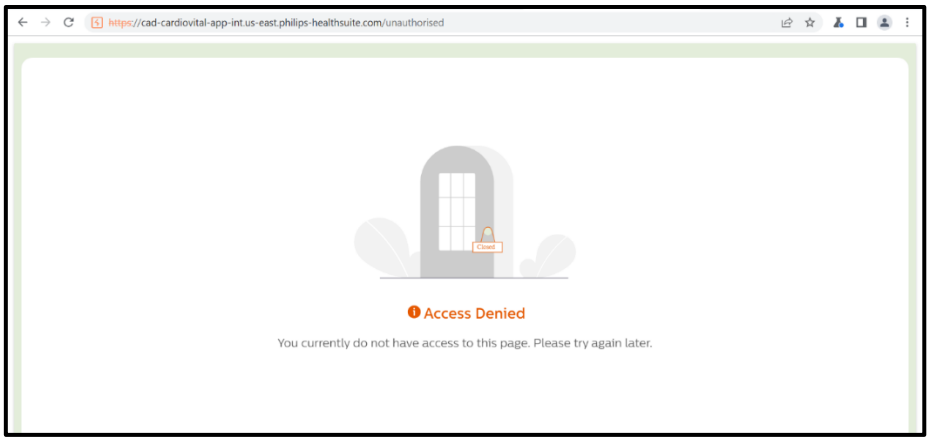
https://docs.philips.com/:v:/g/personal/chaitran_shivayogimath_philips_com/EU4LUJeoLGJGtogSQ0QJfjEBv8cjUEeWhVkOEg_ZFjel5w?e=ULvMuz

Retest Status as of 10 Feb 2023:

It is observed that the Instance 1 is still reproduceable as seen in the screenshot below:



The Second instance is fixed as shown below:



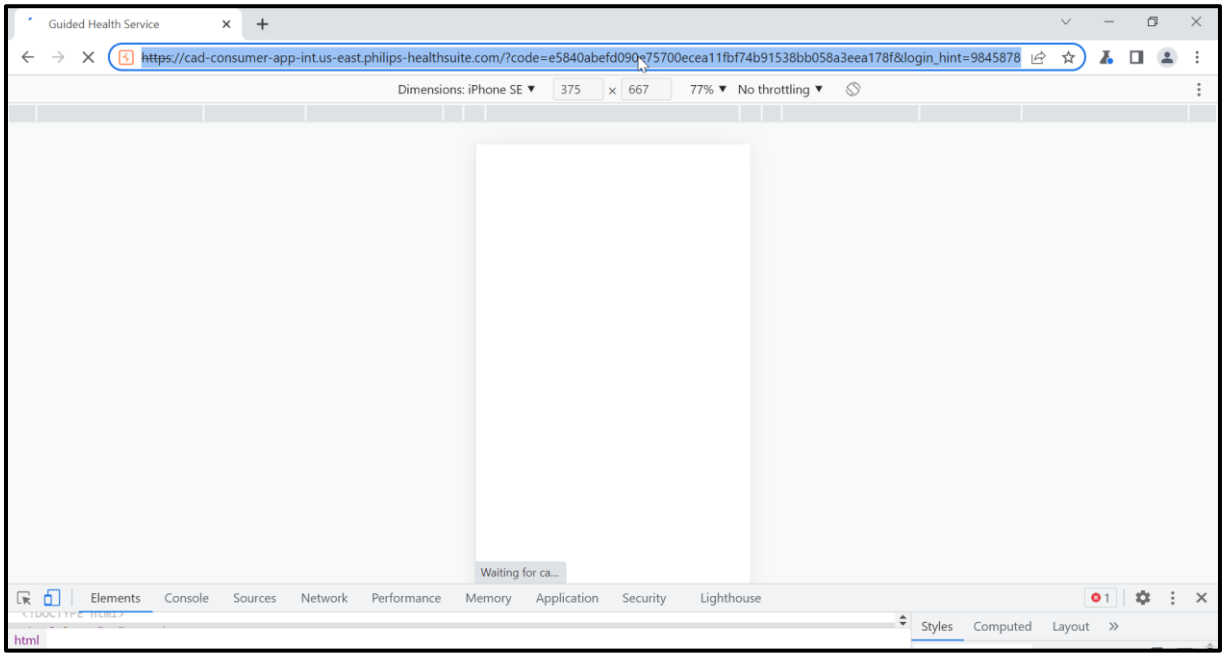
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

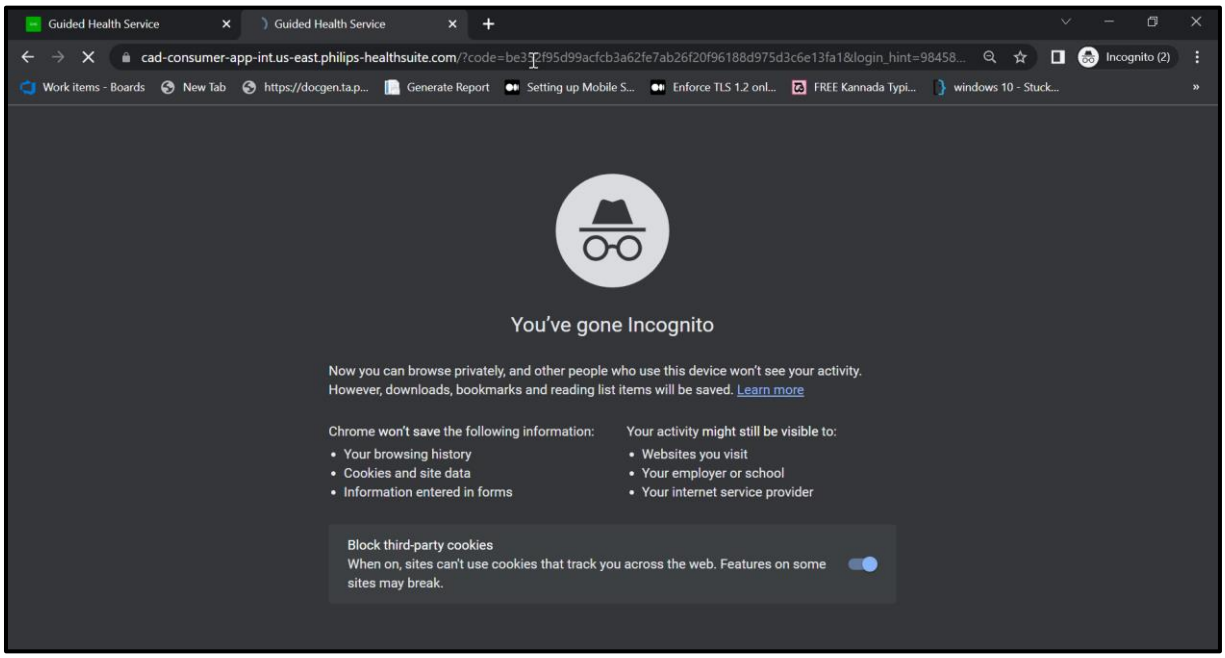
Printed copies are uncontrolled unless authenticated.

There is another instance:

https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=8545169a917ede5f8b84bf03b1ef3be556a2b6917c824c6346&login_hint=9916337921

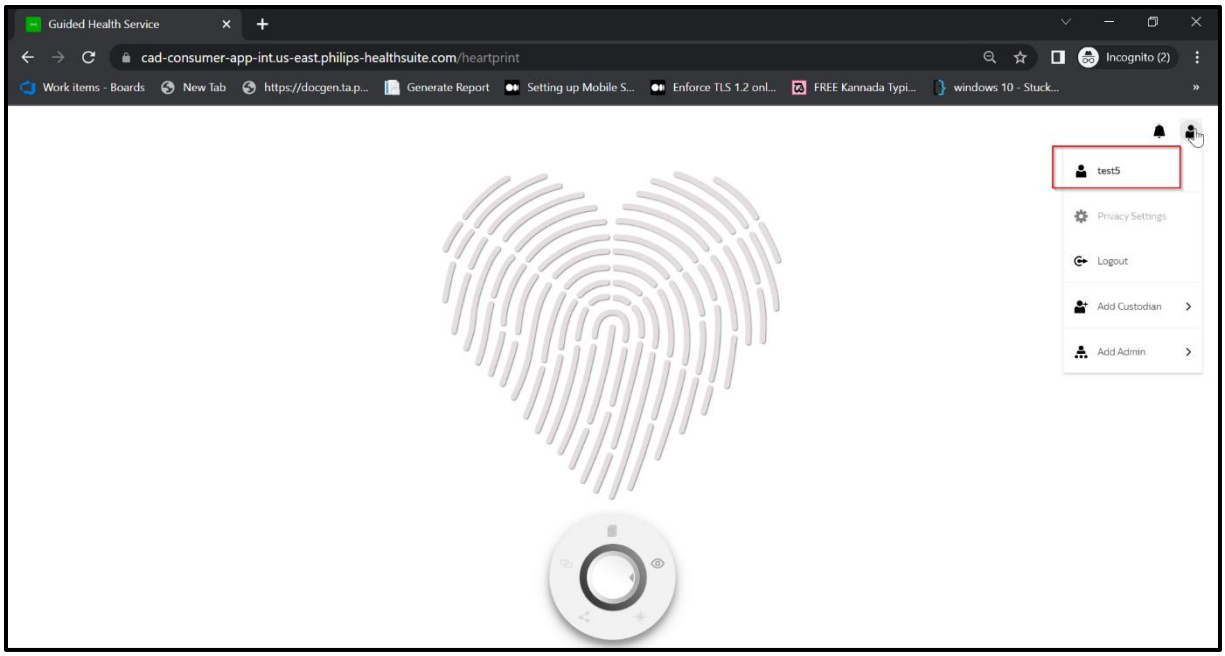
POC:





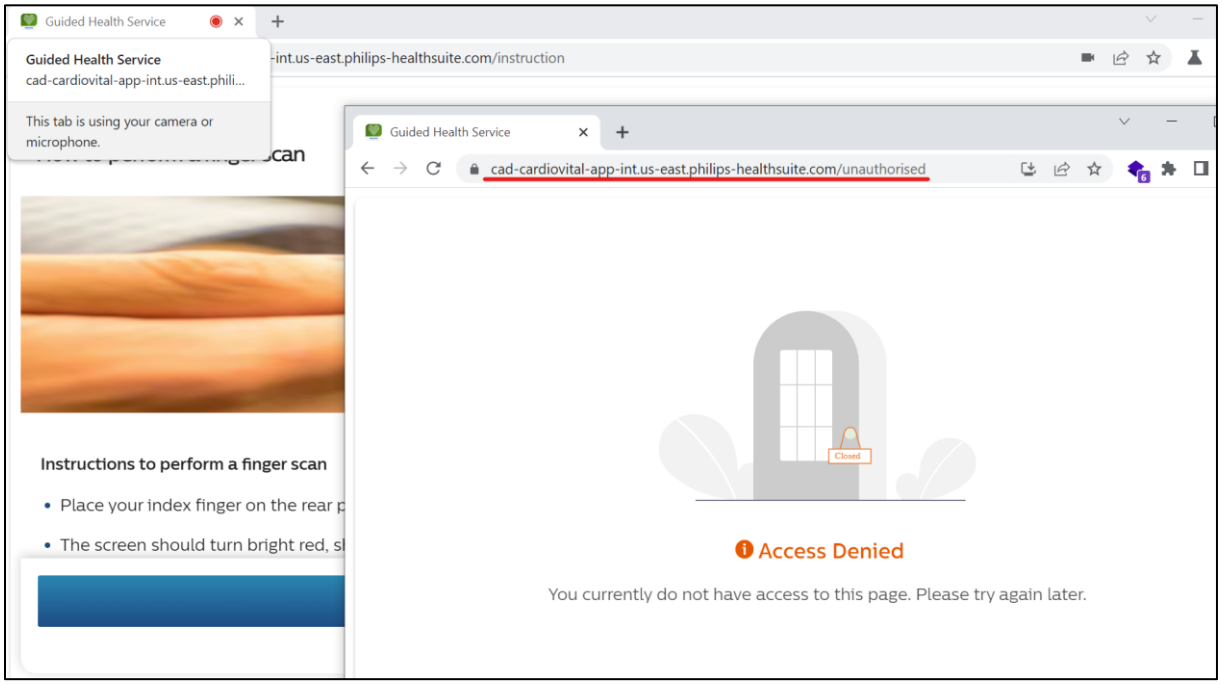
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Resolution (17/April/2023):

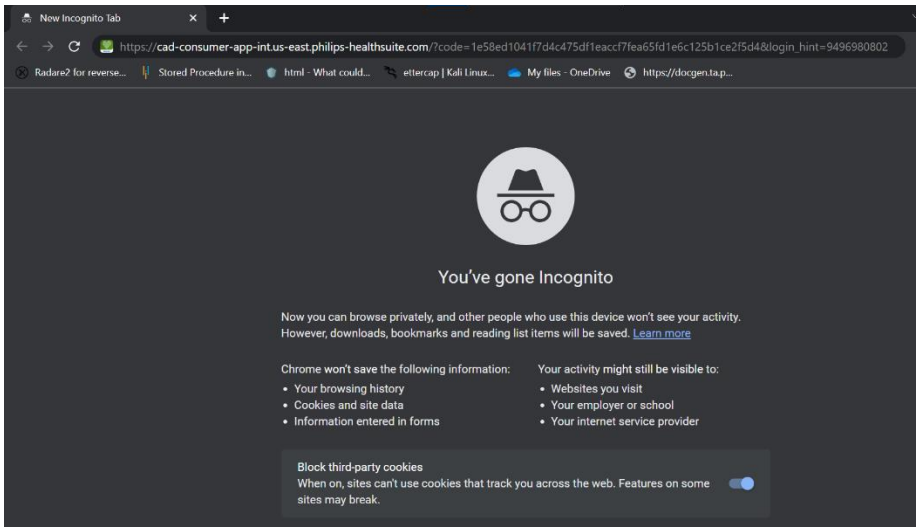
Instance 1:

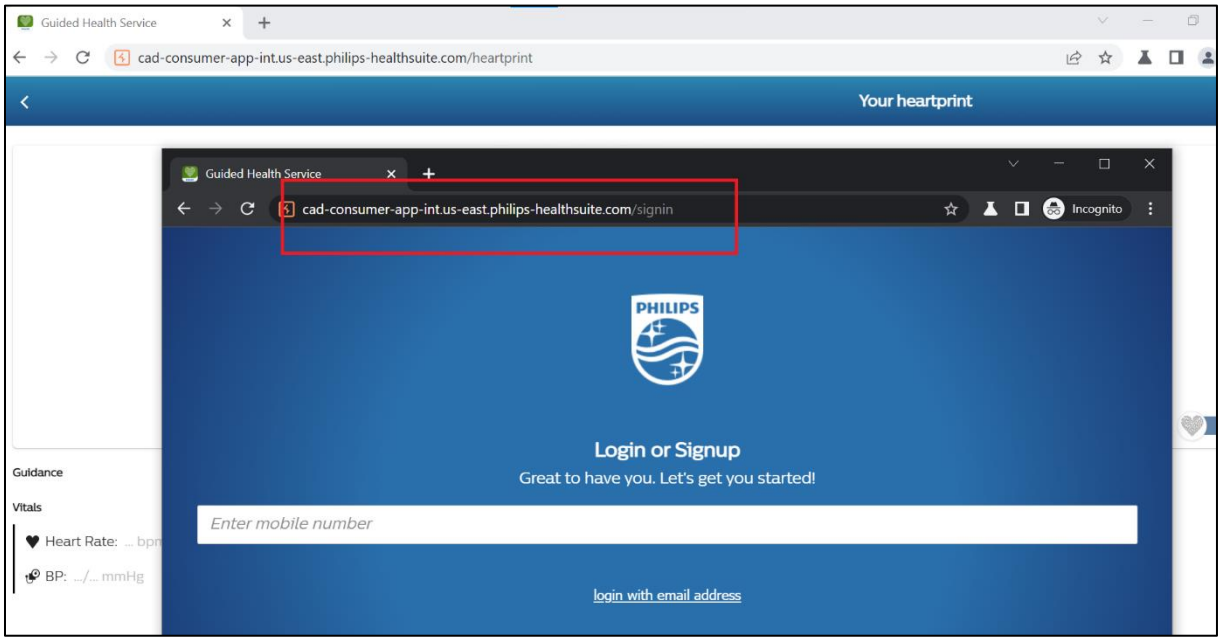


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Instance 3:

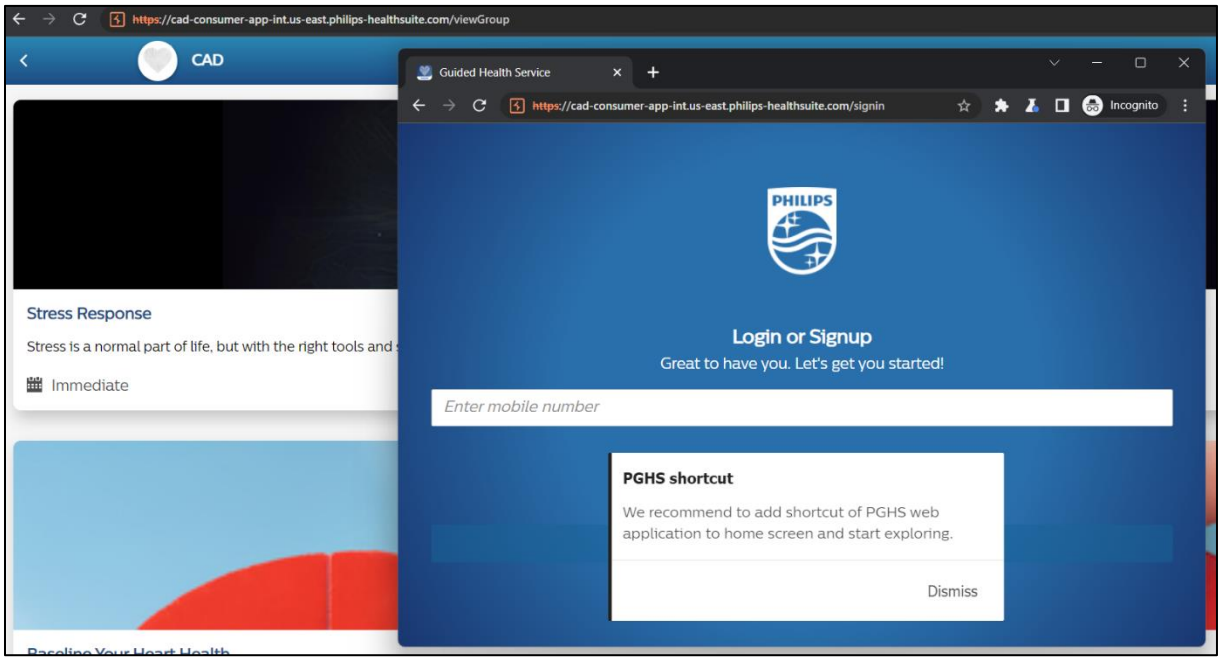




This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



Authentication failed issue is fixed.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.3 Webapp: Modifiable Redirect URI Parameter

Vulnerability Title	Modifiable Redirect URI Parameter
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
Description	**Vulnerability Description:** During the assessment it was observed that for redirect_uri parameter which is user controllable. That parameter would help attacker to craft a request which would come to attacker hosted domain for user activation. Post which attacker can host that domain which resembles Philips original page, with this UI deception attacker can ask credentials from user and this way an adversary would be able to steal user credentials. **Retest status(17/April/2023):** It is observed that URL whitelisting for redirection is still absent. Hence the issue is OPEN. **Retest status(26/April/2023):** The issue still persists. **Retest status (2/May/2023):** URL whitelisting for redirection has been implemented properly. Hence marking this issue as 'CLOSED'. **Retest as of 24-July-2023:** The issue is fixed. **Exploitability Rational:** Since the URI parameter is accepted from client side and not validated on server side. This makes the attack relatively very easy. Attacker needs to craft request after which for user activation request would come to domain where attacker hosted a malicious page which looks like Philips website page. Having a similar character domain name victim can be fooled and hence make user believe on the fake URL. After this user enters credentials which would go to attacker and hence user account could be compromised.

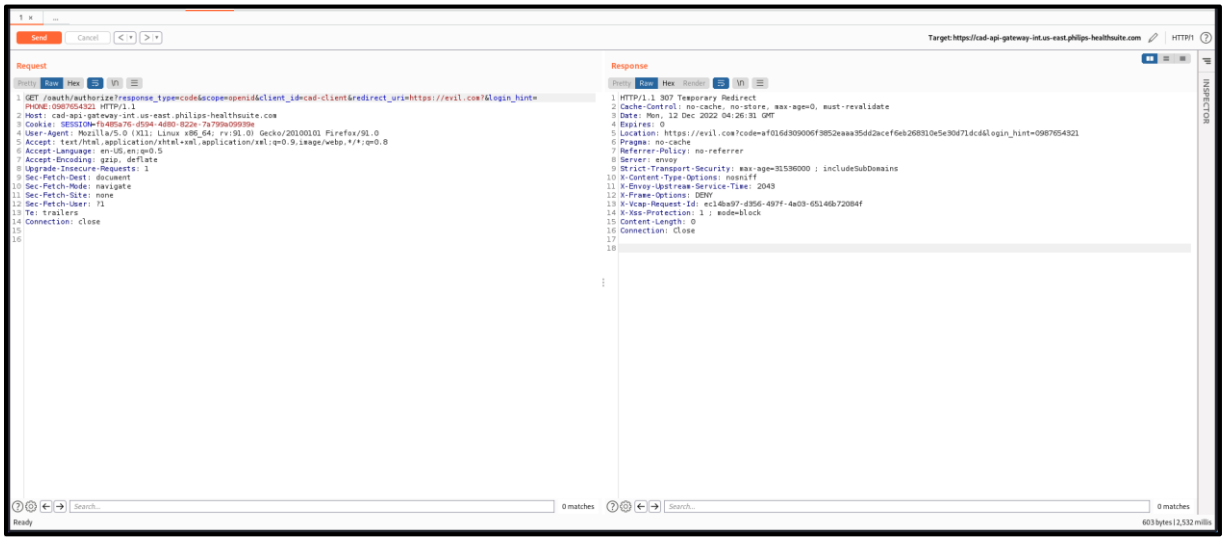
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Impact Rational: This would lead to user account compromise without much efforts from attacker. If user is using same password for other accounts & services then all such accounts could be impacted.
Affected Systems/IP Address/URL	https://cad-api-gateway-staging.us-east.philips-healthsuite.com/oauth/authorize?response_type=code,token,id_token&scope=openid&client_id=cad-client&redirect_uri=https://cad-consumer-app-staging.us-east.philips-healthsuite.com&login_hint=PHONE:9496980802&code_challenge=EUJnz05bd7FTk3IdKN0-gHi87o8RyYyRSz_K8oUKI4k&code_challenge_method=SHA256
Recommendation	It is recommended to use URI parameter from whitelisted one, which is added by developer and not accepting it from user side.
Status	**Closed**

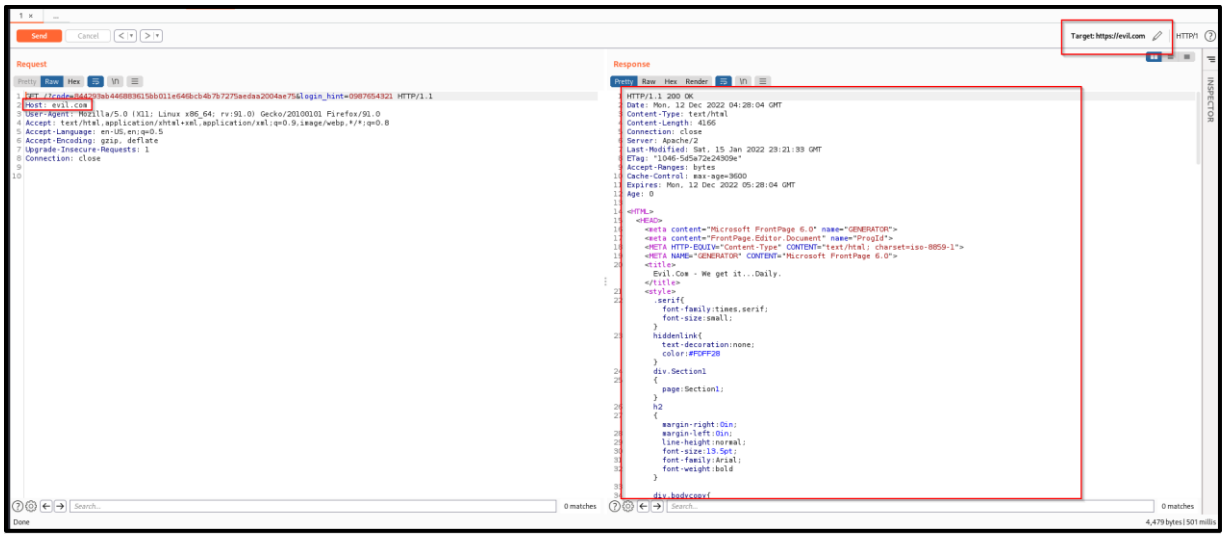
Steps to Reproduce:

1. Configure browser to any proxy tool like burp.
2. Capture the oauth request with redirect_uri parameter.
3. Modify the parameter to any other Domain and it is observed that the redirect_uri can be modified and it redirects the user to the user supplied Domain.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

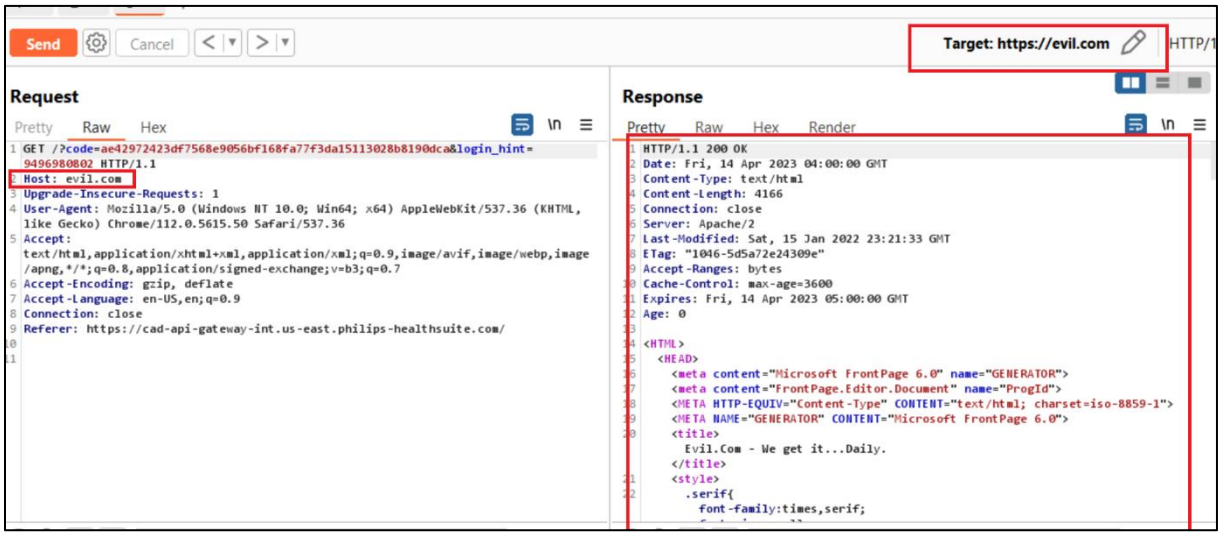
Printed copies are uncontrolled unless authenticated.

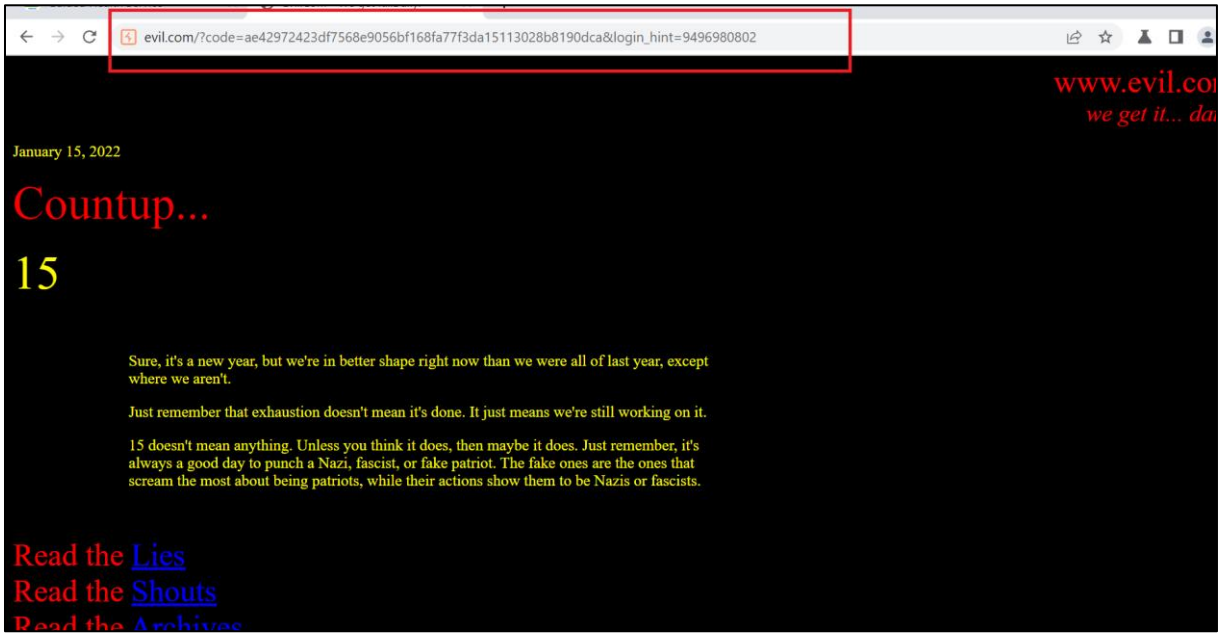


Retest status as of 14 April, 2023:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.





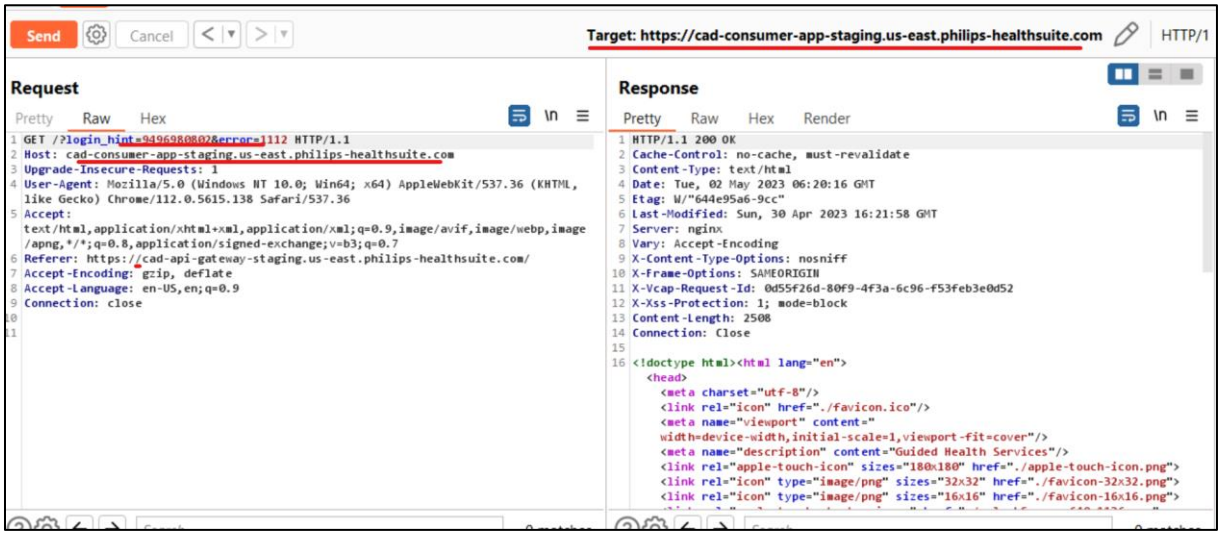
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest status as of 26 April, 2023:

Please refer the [Video POC]

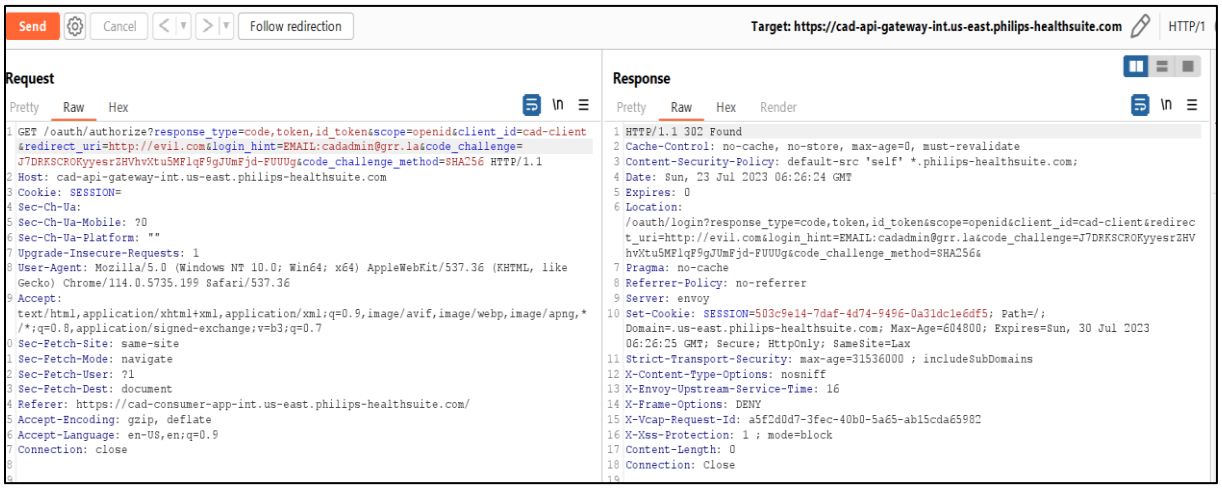
Retest status as of 2 May, 2023:



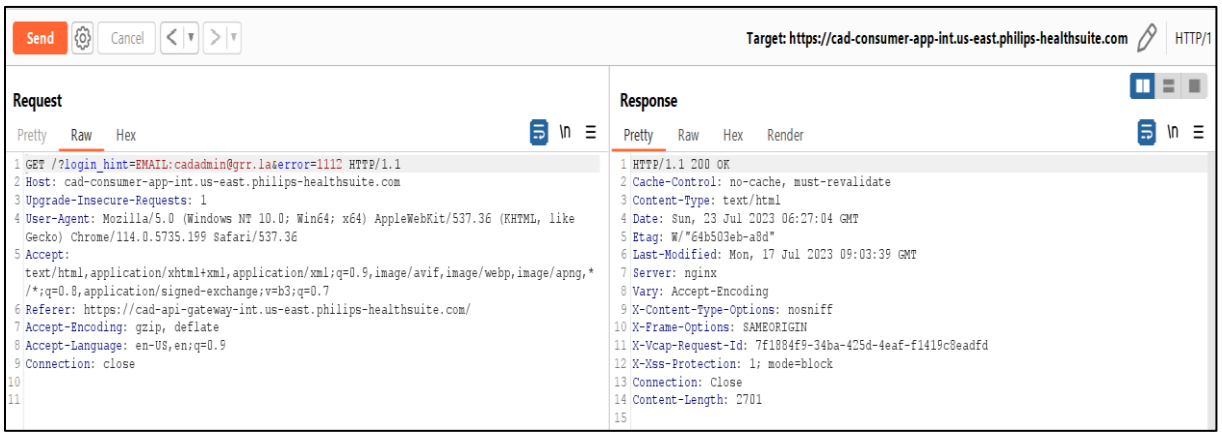
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



Fixed Redirect issue



The issue is fixed

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.4 Webapp: Rate Limiting Not Implemented

Vulnerability Title	Rate Limiting Not Implemented
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Description	**Vulnerability Description:** During security assessment it is observed that the application has not implemented Rate Limiting on Resend OTP request. Rate limiting is the process of controlling traffic rate from and to a server or component. It can be implemented on infrastructure as well as on an application level. Here the application does not implement rate limiting. **Retest Status:** It was observed that once the Request OTP request is sent for multiple times in a given time, the OTP will be recieved continously after a long gap, we see a 200OK. When a legitimate user tries to login again, he will not be able to login as the server says Invalid OTP. As seen in the screenshots below. This causes a DOS to a legitimate user. **Note**: This is applicable to Custodian and Admin Login for email ids (Email Flooding). **Retest Status(13/April/2023):** It was observed that rate limit is still missing and causes DOS to a legitimate user when s/he tries to log in. Hence the issue is OPEN. **Retest Status (05/May/2023):** It was observed that rate limit is implemented in such a way that OTP enabling happens only for three times and then the functionality is blocked for 10 mins. This prevents DOS attack and hence marking this issue as 'CLOSED'. **Retest as of 24-July-2023:** The issue is fixed.

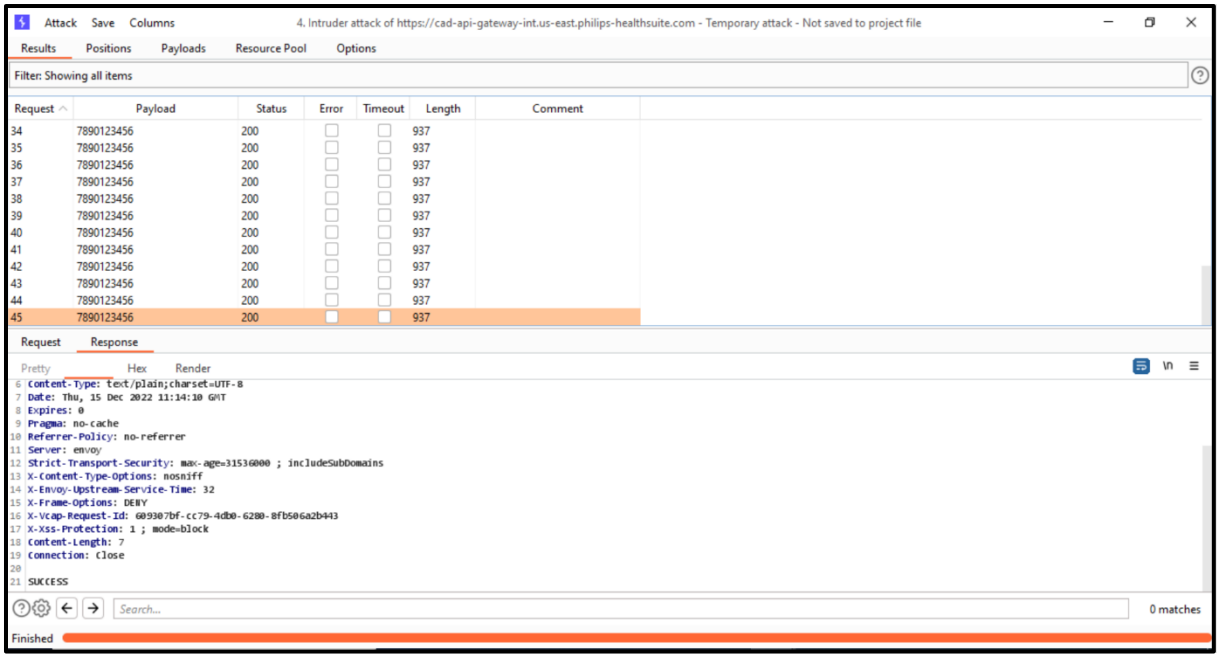
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Exploitability Rational: An attacker who has access to the application URL and Valid user phone numbers/email ids. **Impact Rational:** As an impact, an attacker can send n number of requests to Resend OTP and availability of the server can be compromised and SMS/email can be flood to the end user.
Affected Systems/IP Address/URL	https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/otp
Recommendation	It is recommended to implement captcha to the login page which will help in evading the Bruteforce attacks and multiple requests being sent to the SMS Gateway.
Status	**Closed**

Steps to Reproduce

1. Capture the Resend OTP request using any proxy tool like Burp.
2. Send the request to Intruder and repeat to send this request many times.
3. It is observed that the request can be sent many times.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

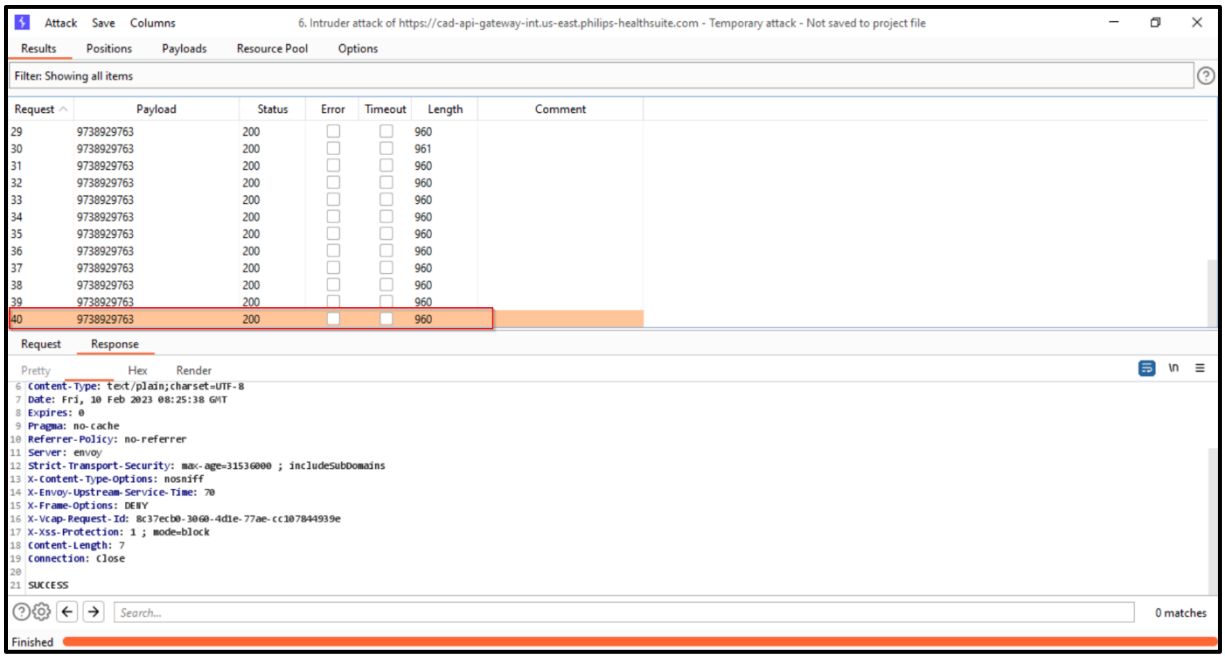
Retest Status as of 10 Feb 2023:

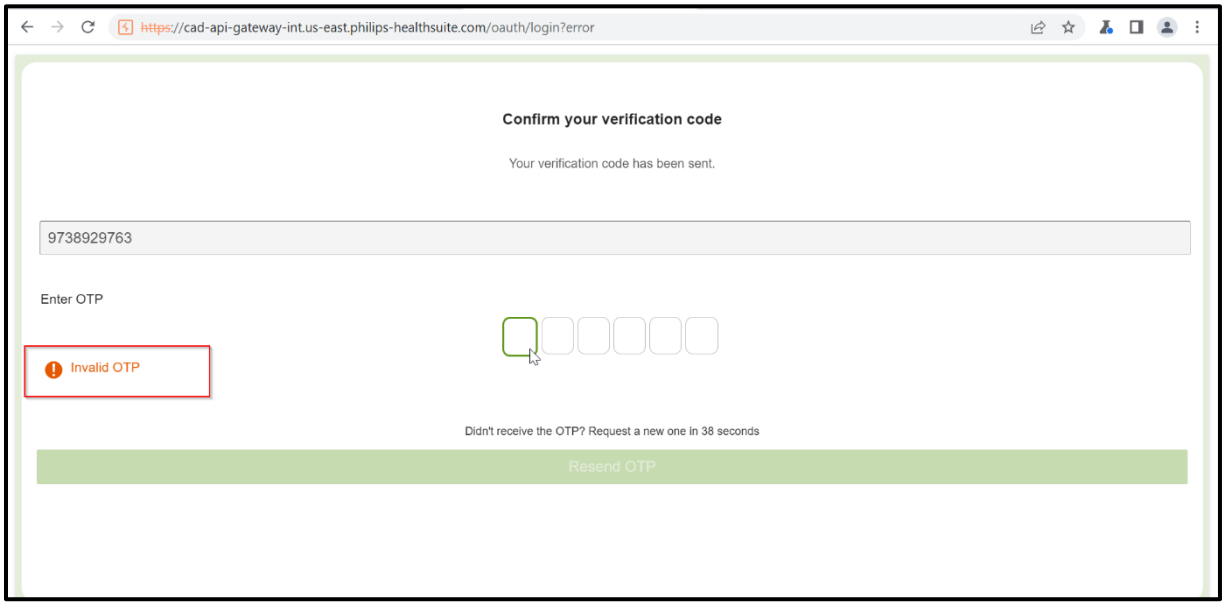
It was observed that once the Request OTP request is sent for multiple times in a given time, the OTP will be recieved only 2 times but we see a 200 OK.

When a legitimate user tries to login again, he will not be able to login as the server says Invalid OTP. As seen in the screenshots below. This causes a DOS to a legitimate user.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

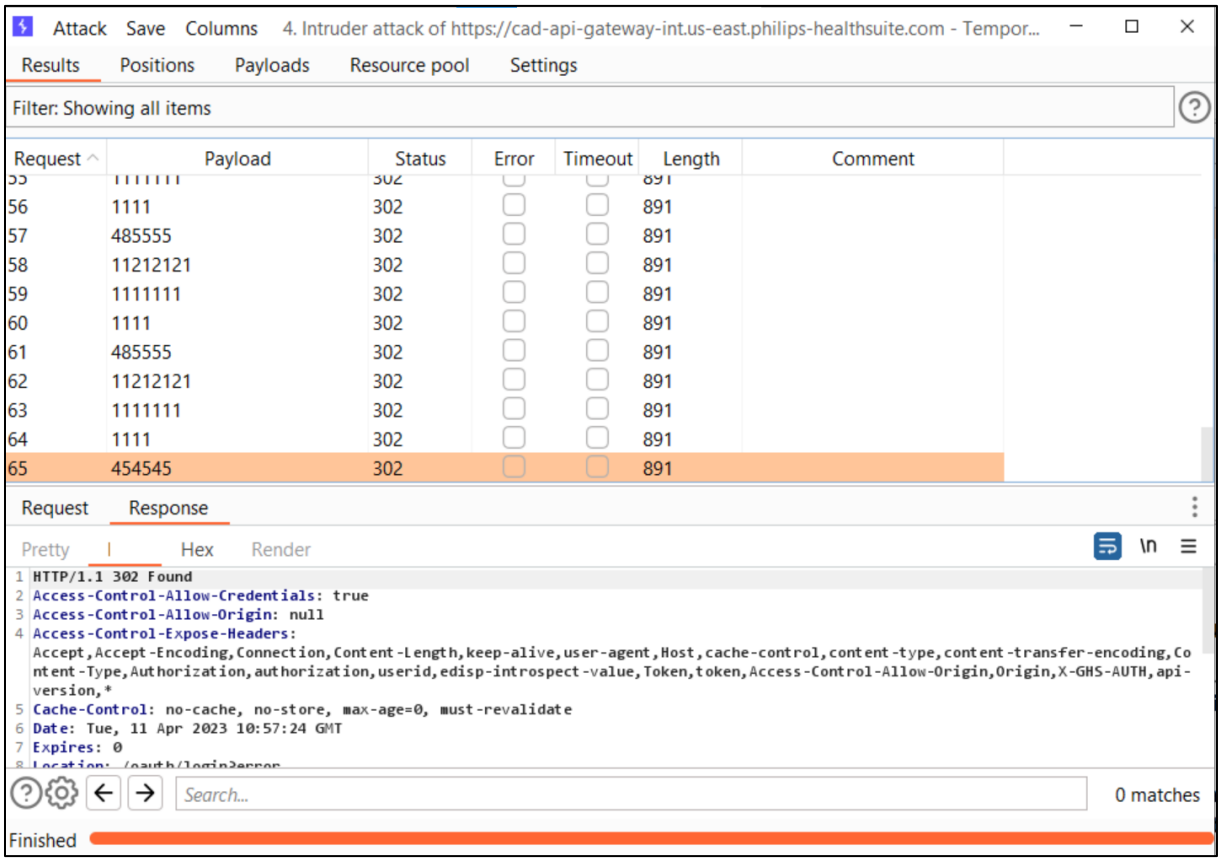




This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

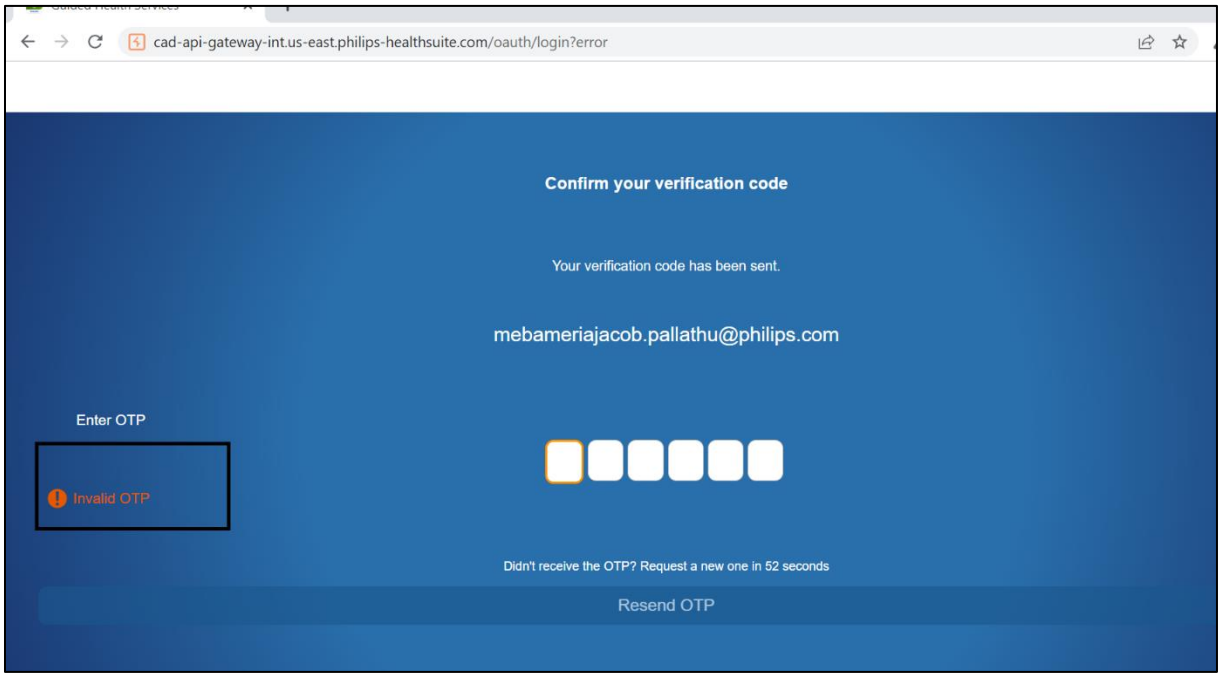
Printed copies are uncontrolled unless authenticated.

Retest status as of 13 April,2023:

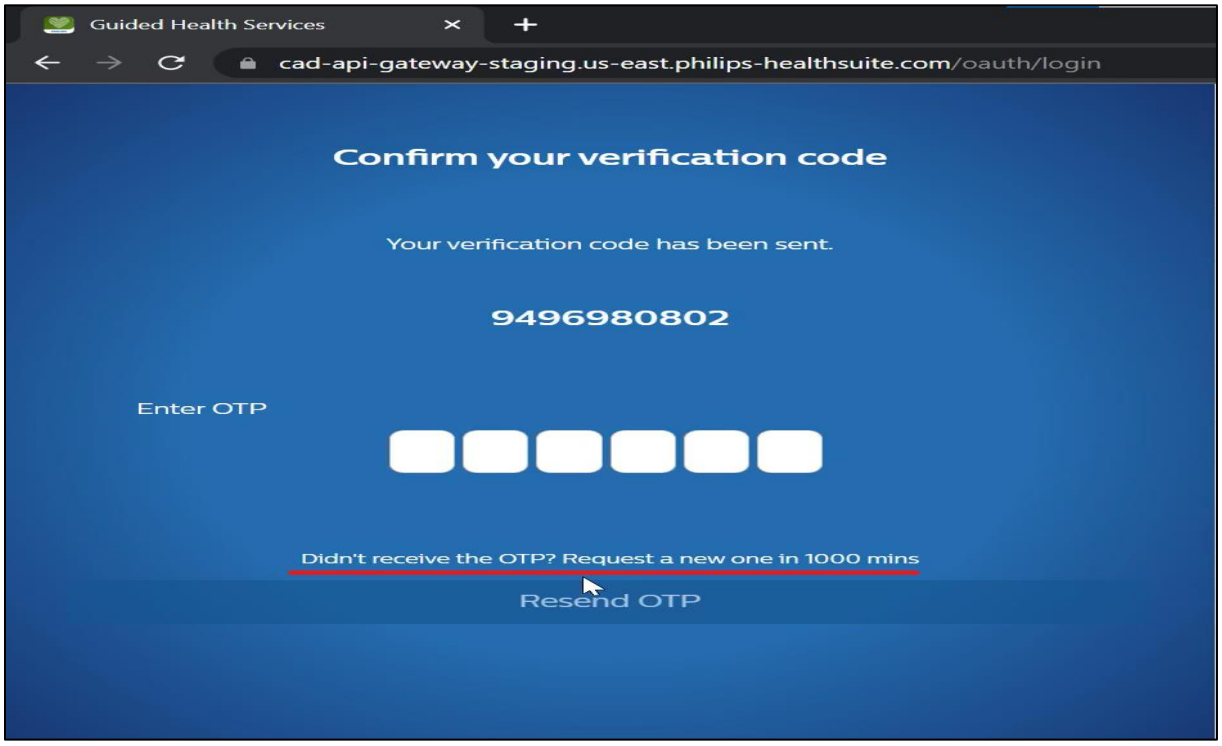


This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



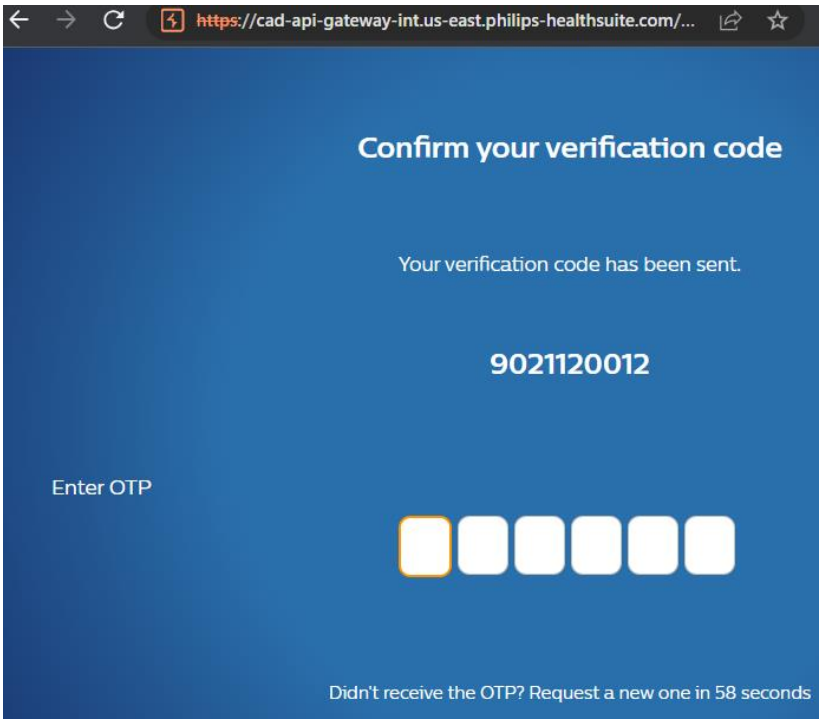
Retest status as of 05/May/2023:



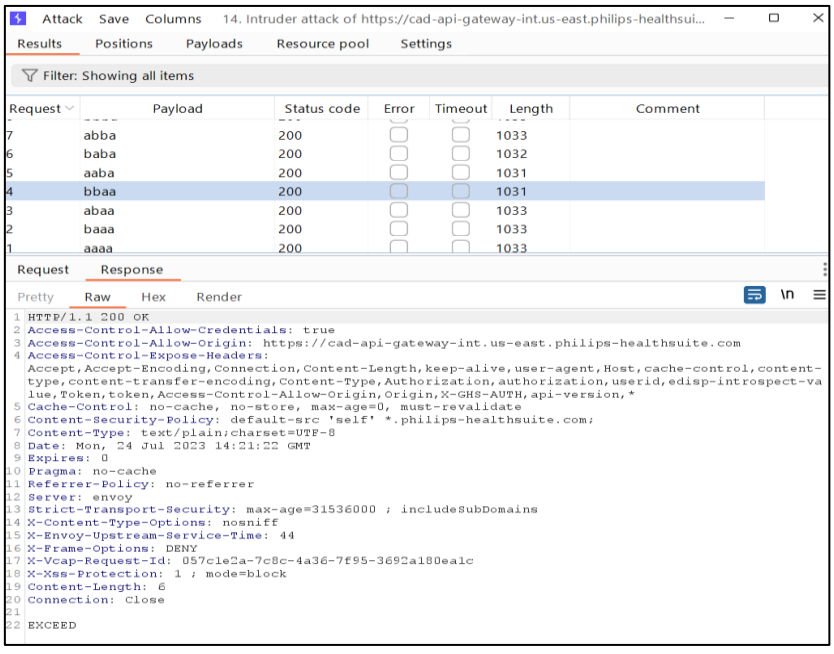
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



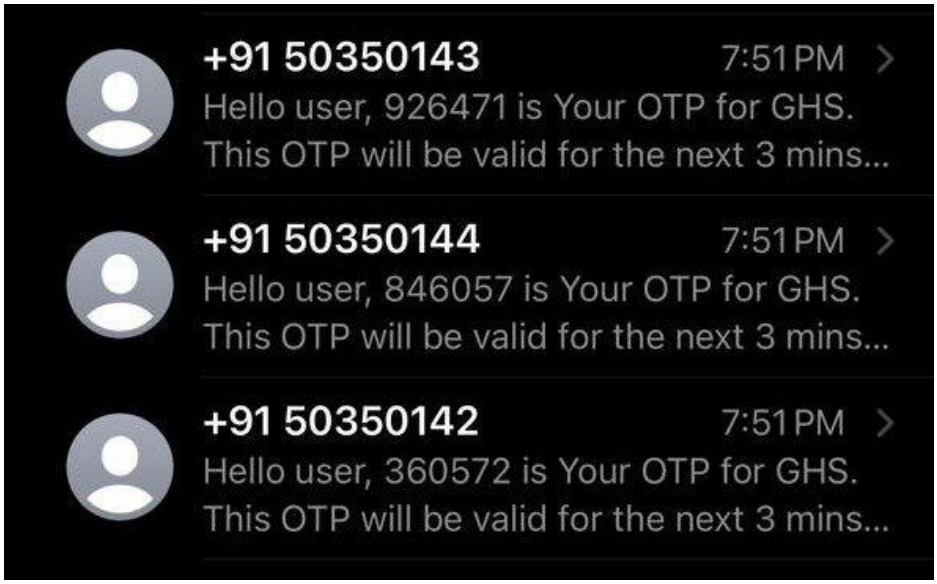
a. Screenshots shows that the attacker tried requesting for OTP to flood victim SMS-inbox



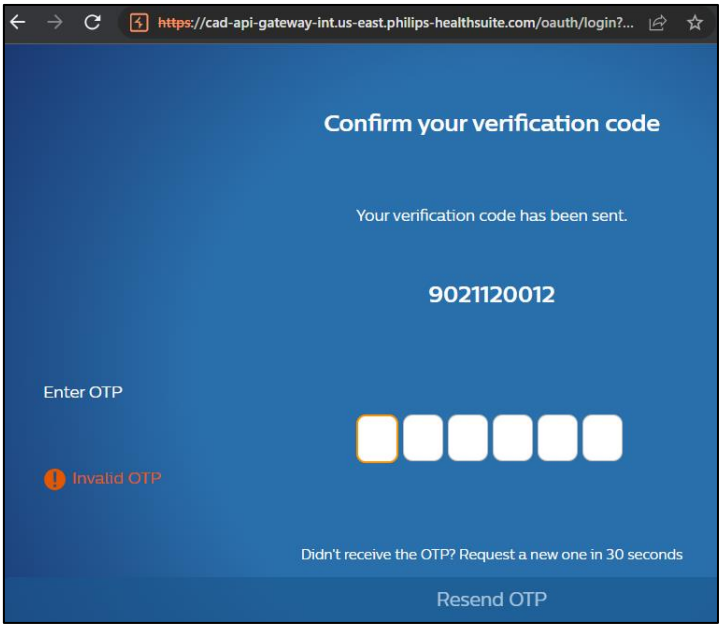
b. Screenshots shows that the attacker used intruder to make OTP flood attack

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



c. Screenshots shows that since rate limiting is enabled, victim will get only 3OTPs



d. Screenshots shows that the Old OTP cannot be reused within 4minutes

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.5 Webapp: Client Side Validation Bypass

Vulnerability Title	Client Side Validation Bypass
Vulnerability Category	A5 Security Misconfiguration
Severity	**Informational**
CVSS V3 Calculation	CVSS Base Score: NA CVSS Vector: NA
Description	**Vulnerability Description:** During the security assessment of the product, it was observed that the Resend OTP button will be disabled for 60s, but it can be bypassed by removing the disabled button and can be enabled any number of times from the application frontend. **Retest status(17/April/2023):** Resend OTP button can be enabled by bypassing the client-side validation. Hence the issue is OPEN. **Retest status (26/April/2023):** The issue still persist. **Retest status(05/May/2023):** It was observed that Resend OTP button can be enabled by bypassing the client side validation but OTP will be sent only for three times and after that, the functionality will be blocked for 10 mins. Hence the severity of this issue is reduced to Observational/Informational. Though we can enable the button, the OTP is triggered only thrice and for next ten mins OTP is blocked. **Retest as of 24-July-2023:** The issue is fixed. **Exploitability Rational:** Any user who has access to Application can exploit this issue. **Impact Rational:** An attacker can send as many Resend OTP requests for any user and availability can be compromised.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://cad-api-gateway-staging.us-east.philips-healthsuite.com/oauth/login
Recommendation	In either cases, it has to be made sure that the Resend OTP button is not enabled unless the desired action is fulfilled. Furthermore, the server should validate if the client side actions fulfill the requirement or not.
Status	**Closed**

Steps to Reproduce

Refer the video POC in the below location:

https://docs.philips.com/:v:/g/personal/chaitran_shivayogimath_philips_com/Ed-XAA2AQPpAusv8mTPCZEkBdlX6cp4H88kw9P0ZVPyIQw?e=frjRlG

Retest status as of 17/April/2023:

https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/EX4dzX35Md5Cmic9_zF1L4QB3HNYy4h5ZuNoain3QUrLIw?e=dWuGDJ

Retest status as of 26/April/2023:

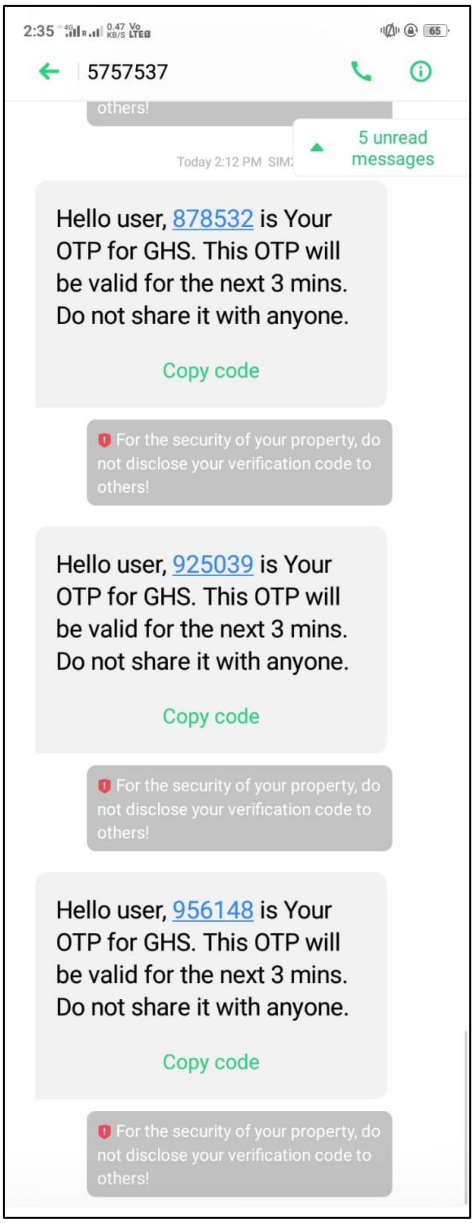
https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/ET37o19XT7lCmM_Ght8uDiABEaEjLhjeQJE5Y4upLRvzoA?e=FuOegw

Retest status as of 05/May/2023:

https://docs.philips.com/:v:/g/personal/mebameriajacob_pallathu_philips_com/EYIs6jHdIBBDlr3vZD_FAIQBRAKc71TD1HGxjarAbssLwQ?e=qw65aV

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

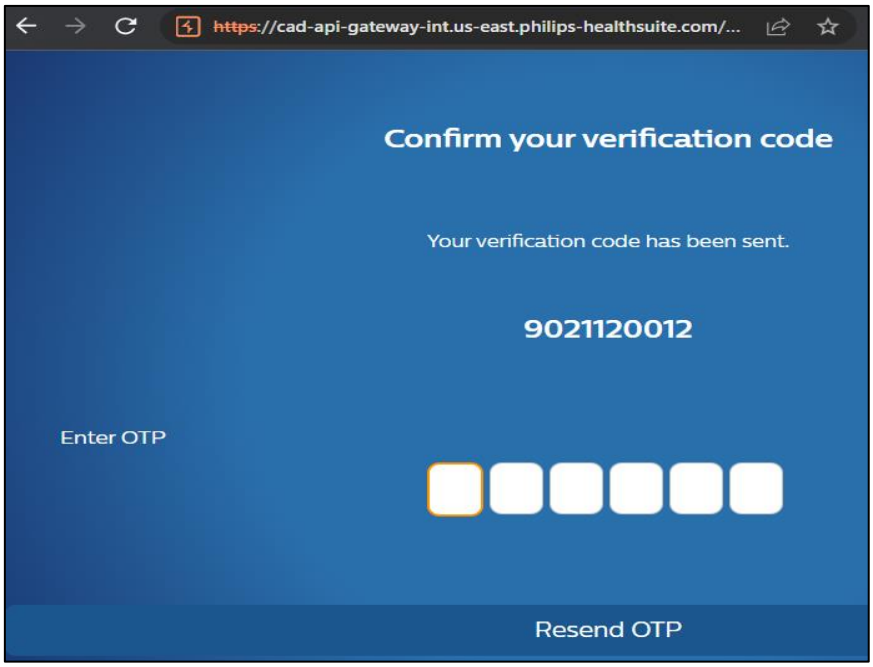
Printed copies are uncontrolled unless authenticated.



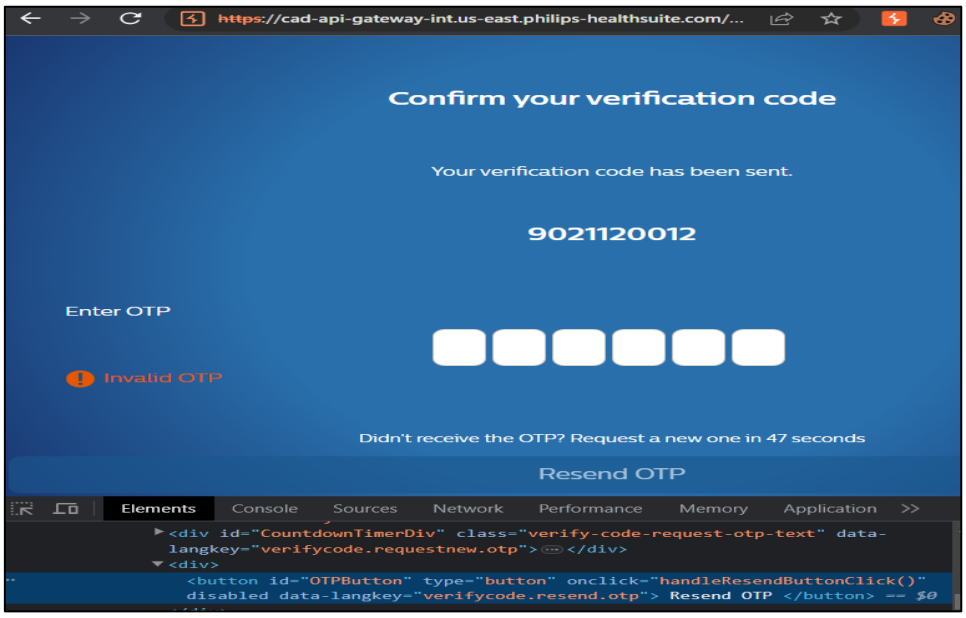
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



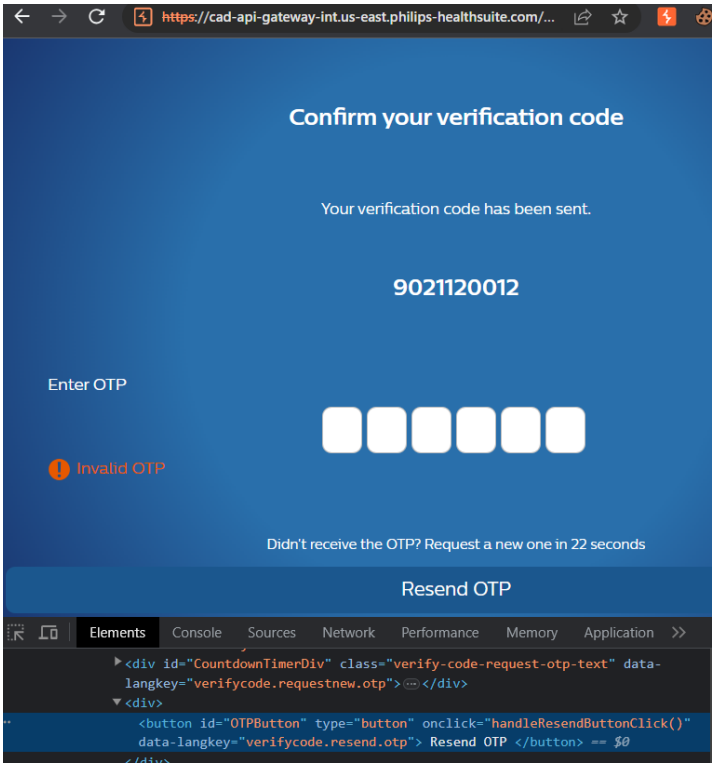
a. **Click on Resend OTP**



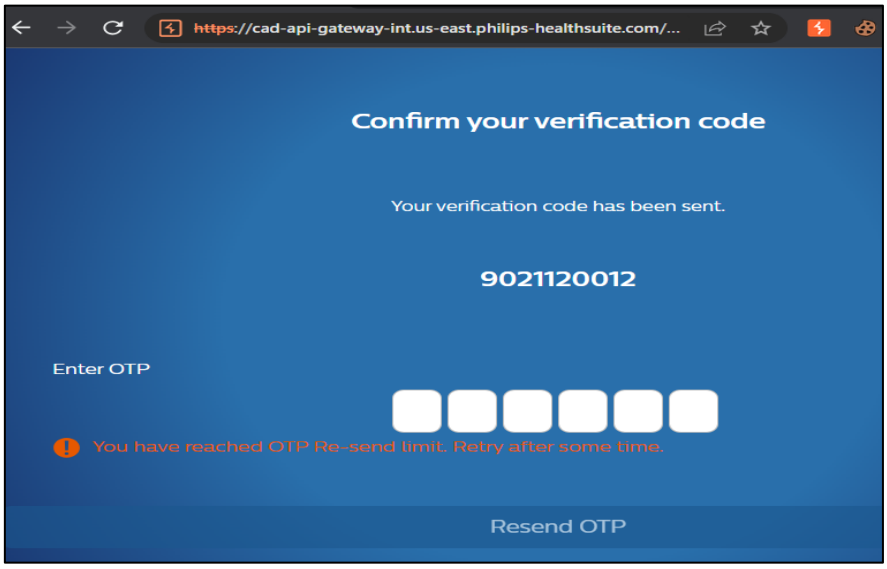
b. Once we clicked, Resend OTP will be disabled

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



c. Try Enabling the Resend OTP option by inspect element, remove Disabled option, and again click on Resend OTP



d. After Resend OTP, Application shows error message like Reached OTP Re-send Limit. From Server end OTP will not be sent to the user.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.6 Webapp: Weak SSL/TLS configuration

Vulnerability Title	Weak SSL/TLS configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 7.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
Description	**Vulnerability Description:** **Case 1,2:** During the security assessment, it was observed that the application supports communication using TLS 1.0 and TLS 1.1. TLS 1.0 has a number of cryptographic design flaws. The server-side SSL/TLS endpoint is configured to allow connections using TLS protocol version 1.0 ("TLSv1.0"), which contains known weaknesses. The TLS protocol provides secure transport between endpoints over a network, with the intended effect of offering data integrity and confidentiality. Certain configurations of TLS version 1.0 are vulnerable to known man-in-the-middle ("MitM") attacks, including the BEAST and POODLE attacks. In addition, multiple standards organizations including NIST and PCI have declared that TLSv1.0 no longer provides sufficient data protection. **Note:** This issue is a High severity issue as per SCoE. Since this is affected by the AWS S3 buckets, which is a known issue and Philips does not have control over the S3 buckets to disable the TLSv1.0 and 1.1 support we are reporting it as a Medium Severity issue. The Product team should approach Amazon to disable the TLSv1.0 and 1.1 support. **Case 3:** One of the TLS/SSL certificates used by your server is about to expire(**Wed Sep 06 2023**). Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server. **Reference:** https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Retest(17/April/2023): AWS S3 buckets are still in use and therefore TLS 1.0 and TLS 1.1 are being used for the communication. Hence the issue is OPEN. **Case 1,2:** **Retest as of 24-July-2023:** The issue still exist. **Case 3:** **Test as of on 24 July 2023:** Server certificate is about to expire. Issue is open. **Exploitability Rational:** Weaknesses in TLSv1.0, v1.1 connections may allow an attacker to decrypt traffic passed between a victim's client and the server. **Case 3:** Exploitability can be performed by accessing the webapplication, once the SSL certificate is expired, attacker can perform MITM attacks and capture every request which is send by victim. **Impact Rational:** Any sensitive information passed over this connection may be exposed. **Case 3:** If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.
Affected Systems/IP Address/URL	https://cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com https://cad-api-gateway-int.us-east.philips-healthsuite.com/ https://cad-consumer-app-int.us-east.philips-healthsuite.com/
Recommendation	**Case 1,2:** It is advised to support TLS1.2 and TLS1.3 and disabling older protocols (not supporting for backward compatibility). **Case 3:** Contact your Certificate Authority to renew the SSL certificate.
Status	**Open**

Steps to Reproduce

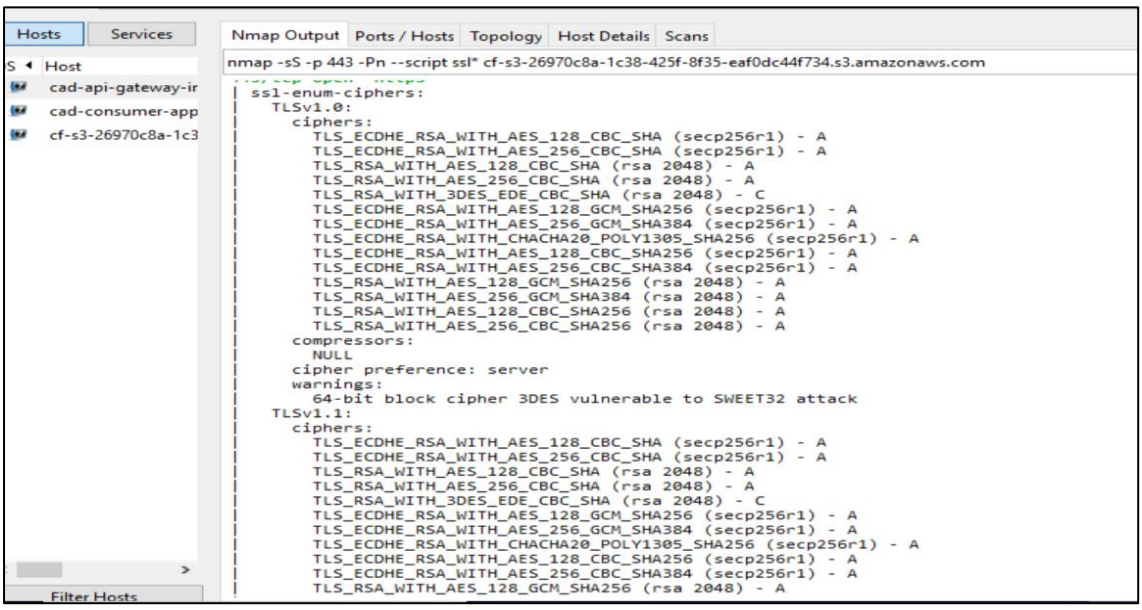
1. Run the sslscan scan by executing the Nmap NSE Scan:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

2. nmap -Pn -sS -p 443 --script ssl* <hostname>

Retest Evidence as of 18 Apr 2023:



Refer section 9 for detailed nmap ssl scan results.

Retest Status as of 24th July 2023

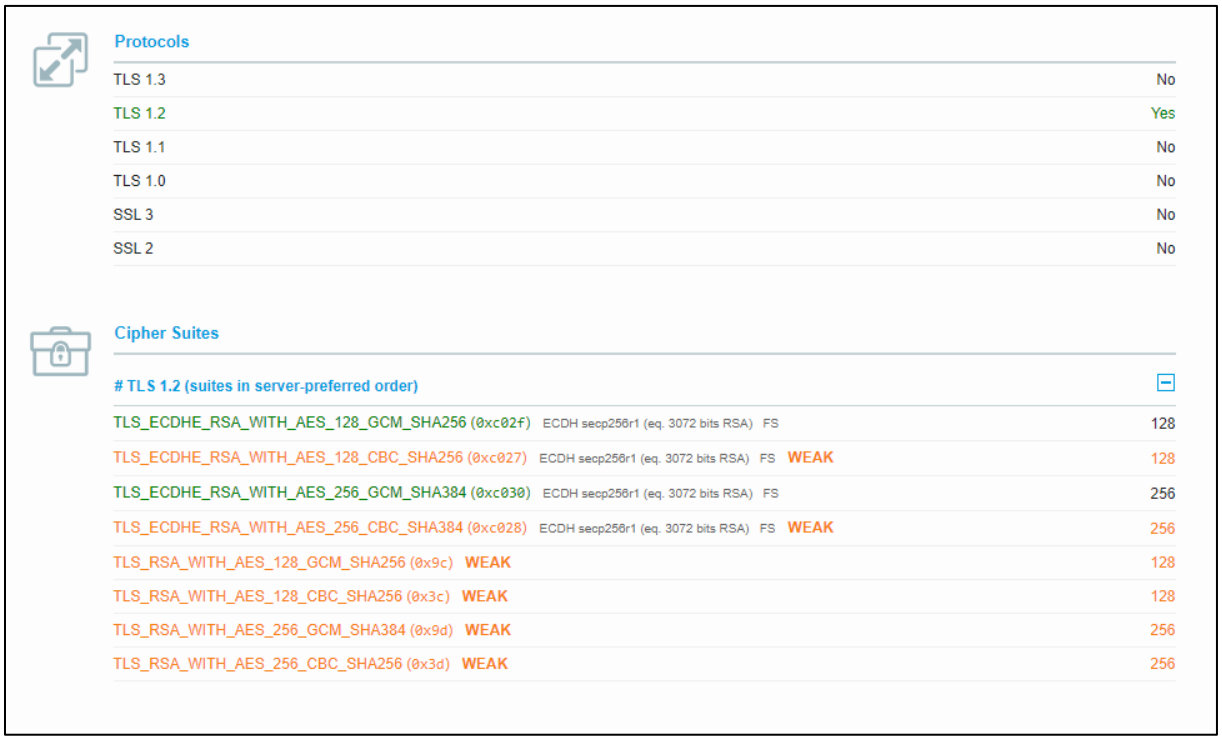
Case 1: https://cad-consumer-app-int.us-east.philips-healthsuite.com/

```
Nmap scan report for cad-consumer-app-int.us-east.philips-healthsuite.com (54.161.119.237)
Host is up (0.0099s latency).
Other addresses for cad-consumer-app-int.us-east.philips-healthsuite.com (not scanned): 52.87.118.180
rDNS record for 54.161.119.237: ec2-54-161-119-237.compute-1.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

Identified Weak TLS CBC Cipher with NMAP Scan

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

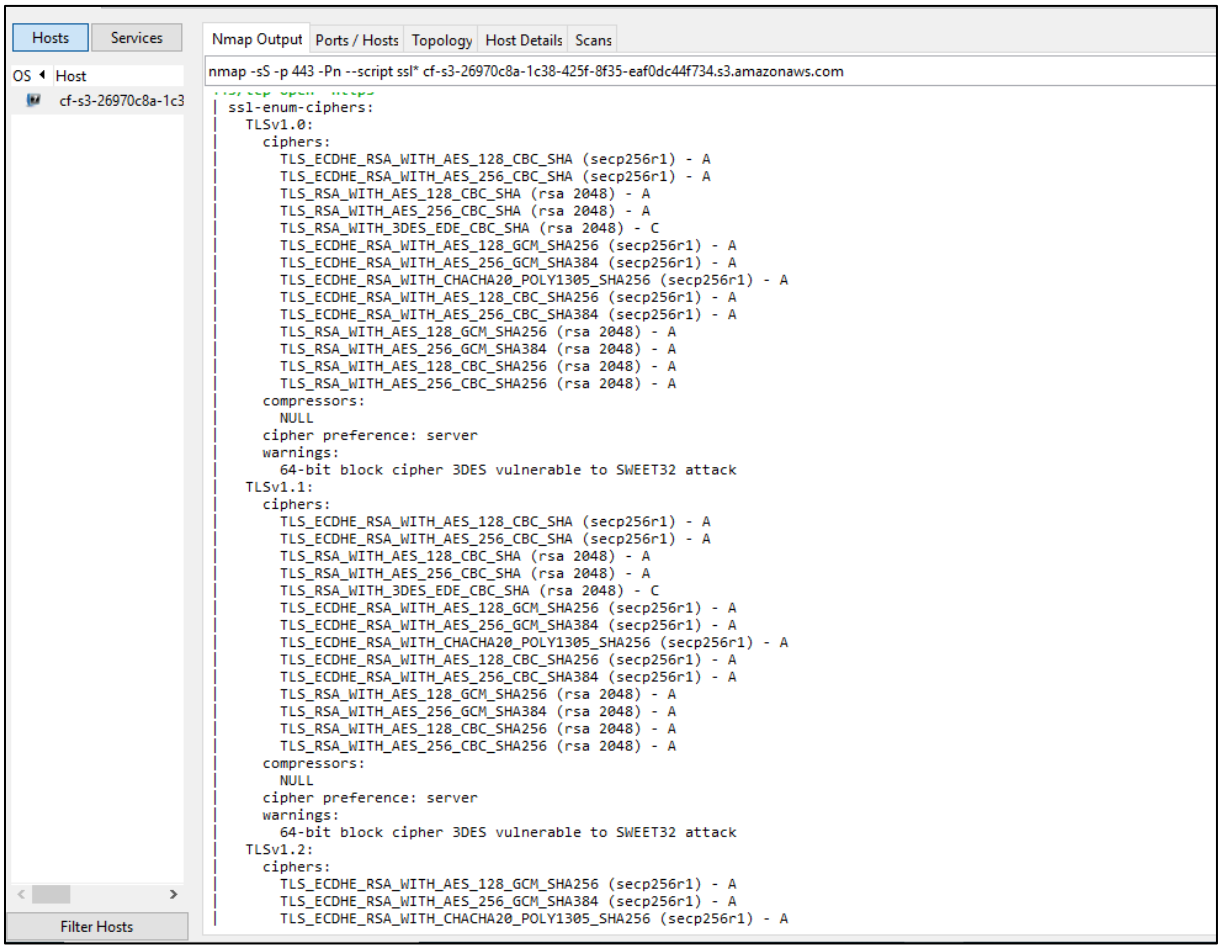


Identified Weak TLS CBC Cipher under SSL Labs Scan

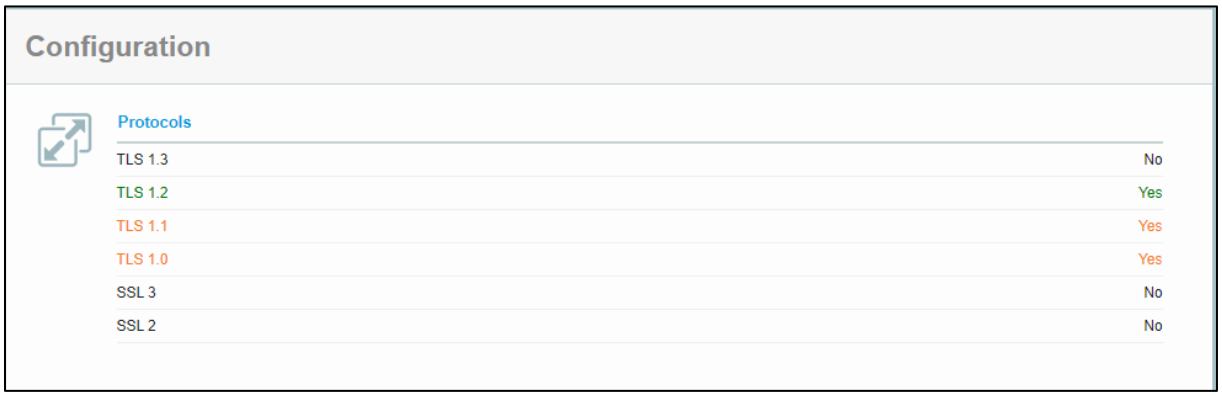
Case 2: https://cf-s3-26970c8a-1c38-425f-8f35-eaf0dc44f734.s3.amazonaws.com

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



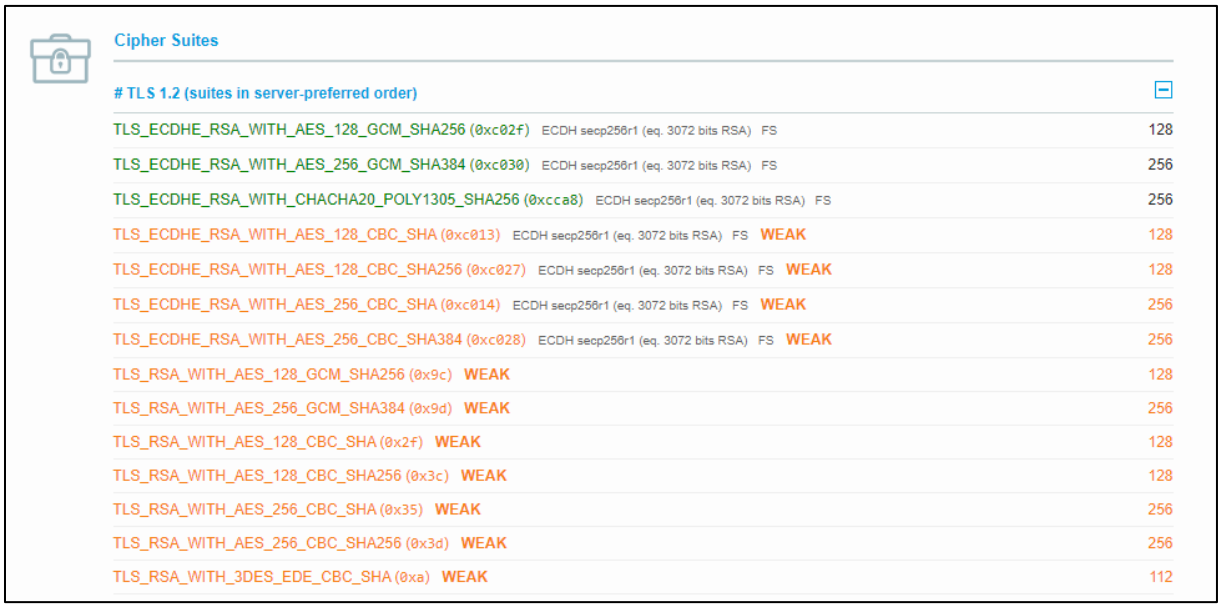
Identified Weak TLS CBC Cipher with NMAP Scan



Identified Weak TLS CBC Cipher under SSL Labs Scan

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

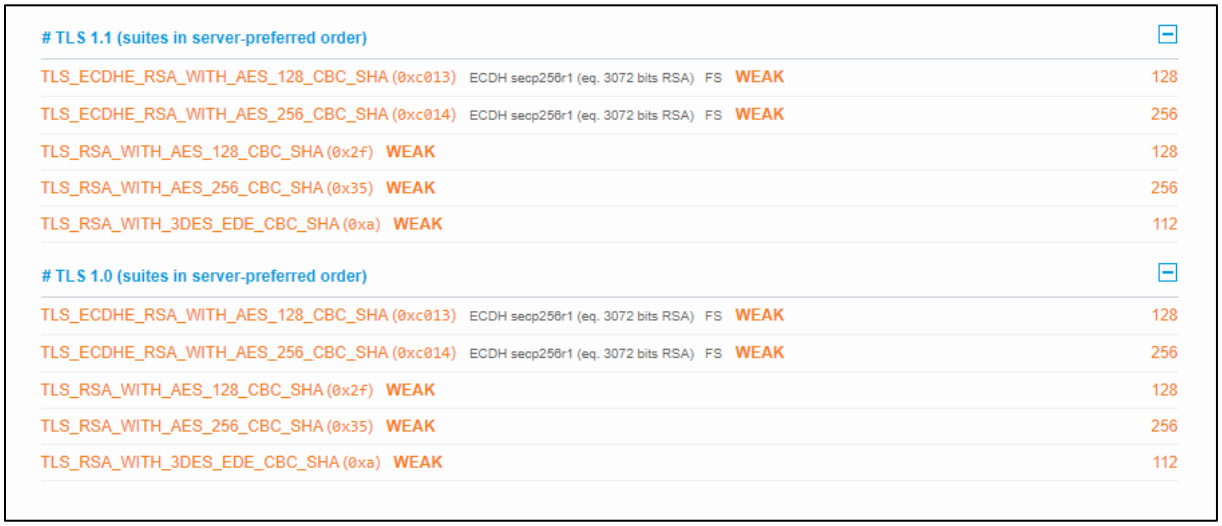


Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK		256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK		112

Identified Weak TLS CBC Cipher under SSL Labs Scan



TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK		112

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK		256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK		112

Identified Weak TLS CBC Cipher under SSL Labs Scan

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Case 3:
Test Evidence as of on 24 July 2023:

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.us-east.philips-healthsuite.com
Altnames: DNS:*.us-east.philips-healthsuite.com, DNS:us-east.philips-healthsuite.com
Issuer:   DigiCert TLS RSA SHA256 2020 CA1

Not valid before: Aug 10 00:00:00 2022 GMT
Not valid after:  Sep  5 23:59:59 2023 GMT
```

Server certificate is about to expire

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.7 Webapp/WebServices: Improper Session Management

Vulnerability Title	Improper Session Management
Vulnerability Category	A7 Identification and Authentication Failures
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 6.1 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N
Description	**Vulnerability Description:** **Case 1:** It was observed that session id is not invalidated at the server side due to which session id of one user can be used for the other user. **Case 2:** The application allows concurrent sessions: It was observed that upon deletion of user account, if the user is already logged in to the application via different browser, the existing session remain alive without any restrictions. Once the user logs out, then that user needs to sign up again to access the application. But until then that user can access and perform all operations. **Case 3**: If there are multiple tabs opened in same browser window and if the user initiates log out in one tab, then it is observed that the other parallel tabs are not automatically brought to login page. (Ideally immediately all tabs for same hostname should be redirected to login page post logout) **Case 4**: It was observed that the application does not log the user out after a reasonable period of inactivity. Inactivity timeout periods vary depending on the sensitivity of the data and functionality the application contains, but idle sessions longer than 15-30 minutes are typically considered vulnerable. **Case 5:** It was observed that if a user has logged into the application and closed the browser without logging out, then if the application is accessed, it is not brought to log in page. The tokens get regenerated and one can perform actions even without the need of log in.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Retest as of 24-July-2023: The issue is still valid and not fixed. **Exploitability rational** For the case 1, attacker should have access to the application. For the case 2, user needs to be logged in to the application. For the case 3, user need to be logged in to the application in two or more different tabs of same browser window. For the case 4 and case 5 to be exploited, the attacker needs physical access to the system. **Impact Rational:** Leaving the user's session active after the user initiates logout provides the attacker with a larger window in which to steal a victim's session and impersonate that user in the application. The session token can be obtained through various techniques, such as intercepting network traffic ("Man-in-the-Middle" or "MitM"), Cross-Site Scripting (XSS), Cross-Site Tracing (XST), and in the case of URL-based session token transmission, local inspection of browser history. In addition to prolonging the session identifier's exposure to attack, failing to invalidate the user's session server-side also leaves the user with no way to deny an attacker's access once the victim discovers that their session has been compromised.
Affected Systems/IP Address/URL	https://cad-consumer-app-int.us-east.philips-healthsuite.com/home https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report
Recommendation	The user's HTTP session should be terminated on the server immediately after a logout action is performed. It is important to note that simply deleting the cookie from the browser will not terminate the server session. The session must be invalidated at the server, using the HTTP container's intrinsic session abandonment mechanism. Reference: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
Status	**Open**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Steps to Reproduce:

Case 1:

Step 1: In 1 browser log in to the application as user A.

Step 2: In 2nd browser, log in as user B.

Step 3: Capture the scan request from 2nd browser.

Step 4: Replace the session id of 'A' with that of 'B'.

Refer the Video POC for more information.

Case 2:

Step 1: Log in to the application in two different browsers.

Step 2: Delete the user account from 1 browser.

Step 3: Observe that the session remains active in the other browser and the user can perform all actions.

Refer the Video POC for more information.

Case 3:

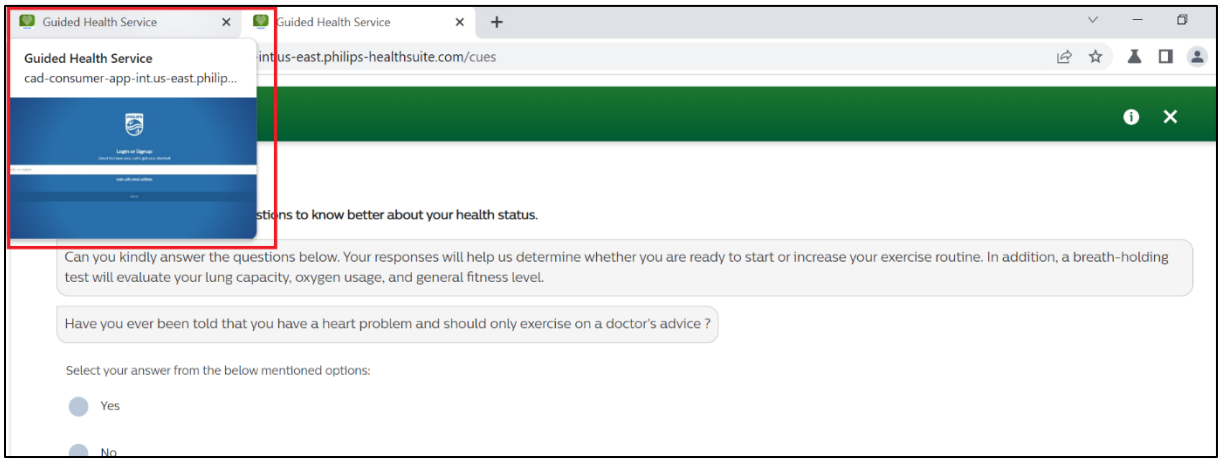
Step 1: Log into the application

Step 2: In the same browser window, log into the application in a different tab.

Step 3: Log out from the application in one tab, observe the adjacent tabs are not brought to the login page. Refer the below screenshot:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

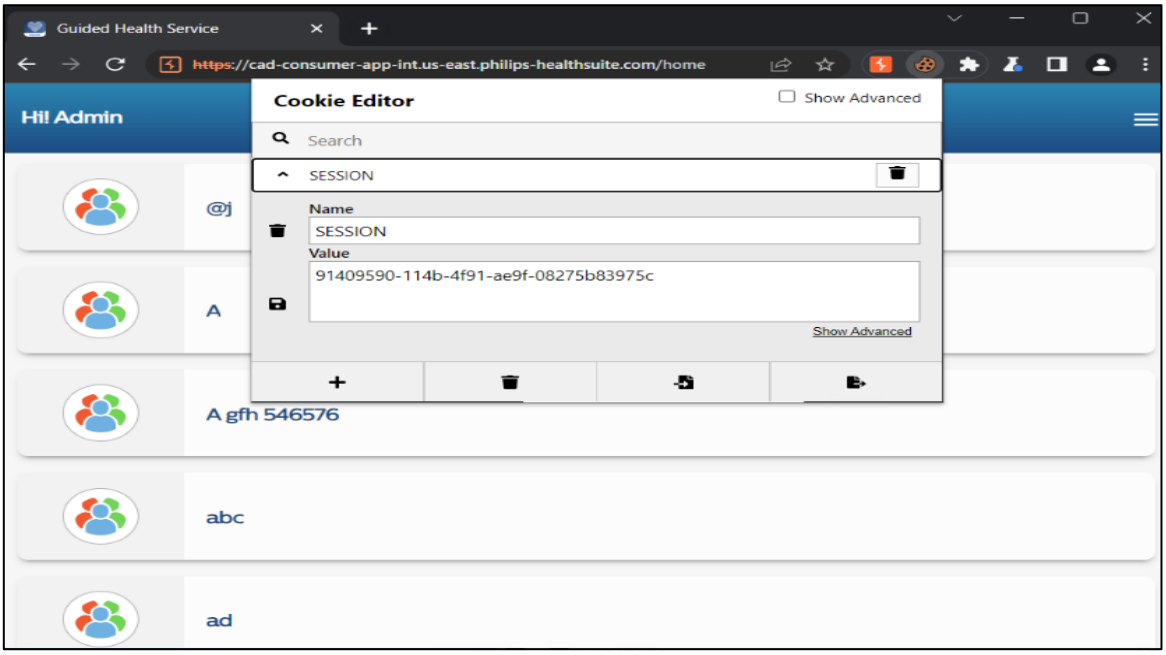


Case 5:

Refer the Video POC for more information

Retest Status as of 24th July 2023:

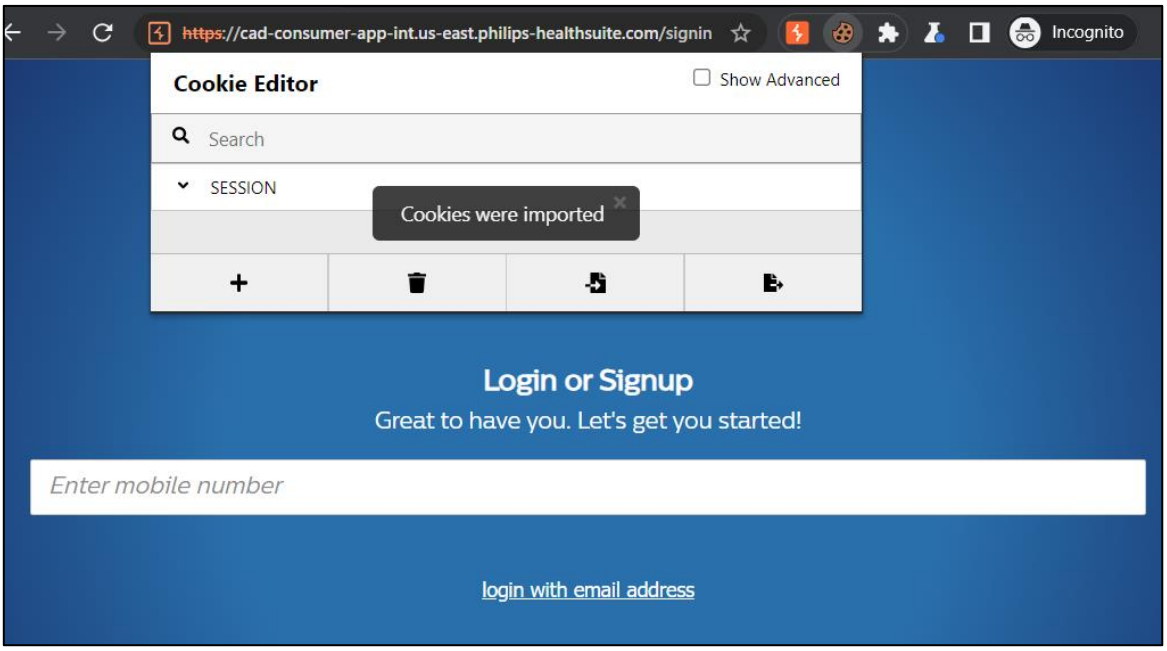
Case 1:



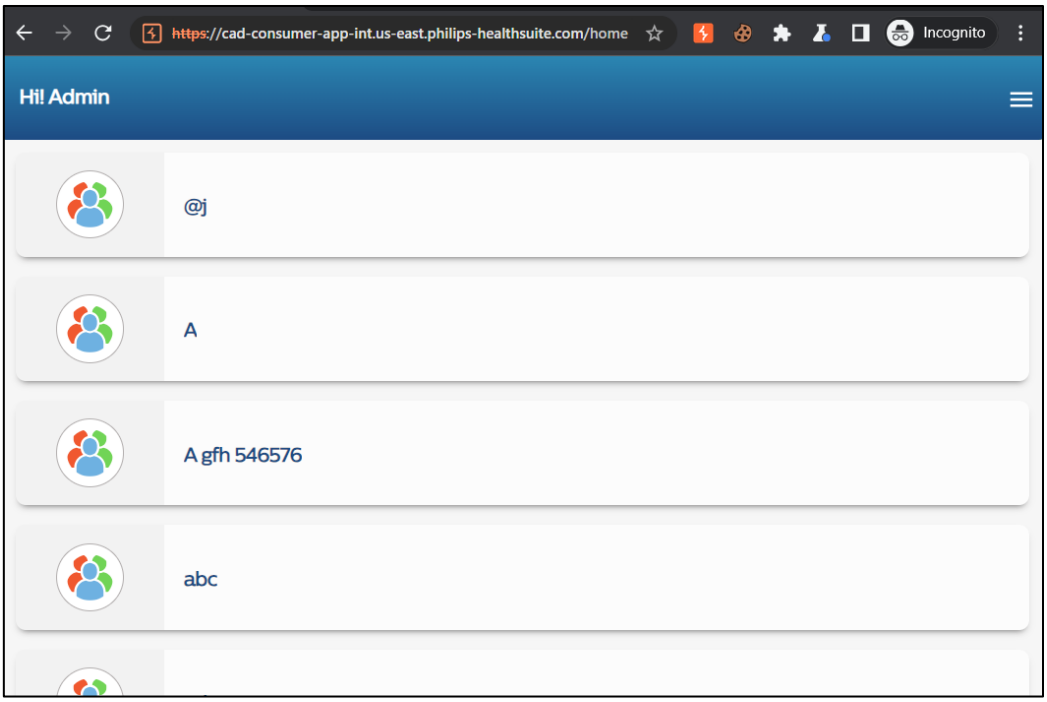
a. Screenshot shows that the Admin session is active in Browser A

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



b. Screenshots shows that the Admin session cookie is imported to Browser B with signin page



c. Screenshot shows that once we refresh the Browser B, we will be login as Admin

Refer the **Video POC**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

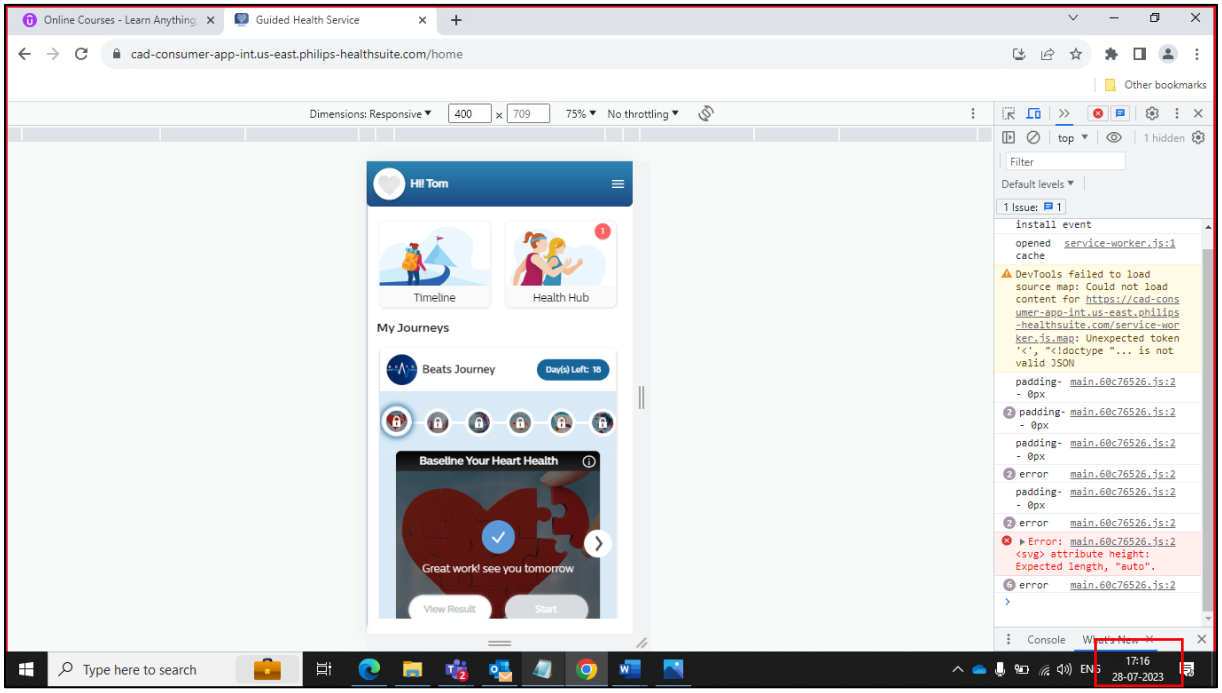
Case 2:

Refer the **Video POC**

Case 3:

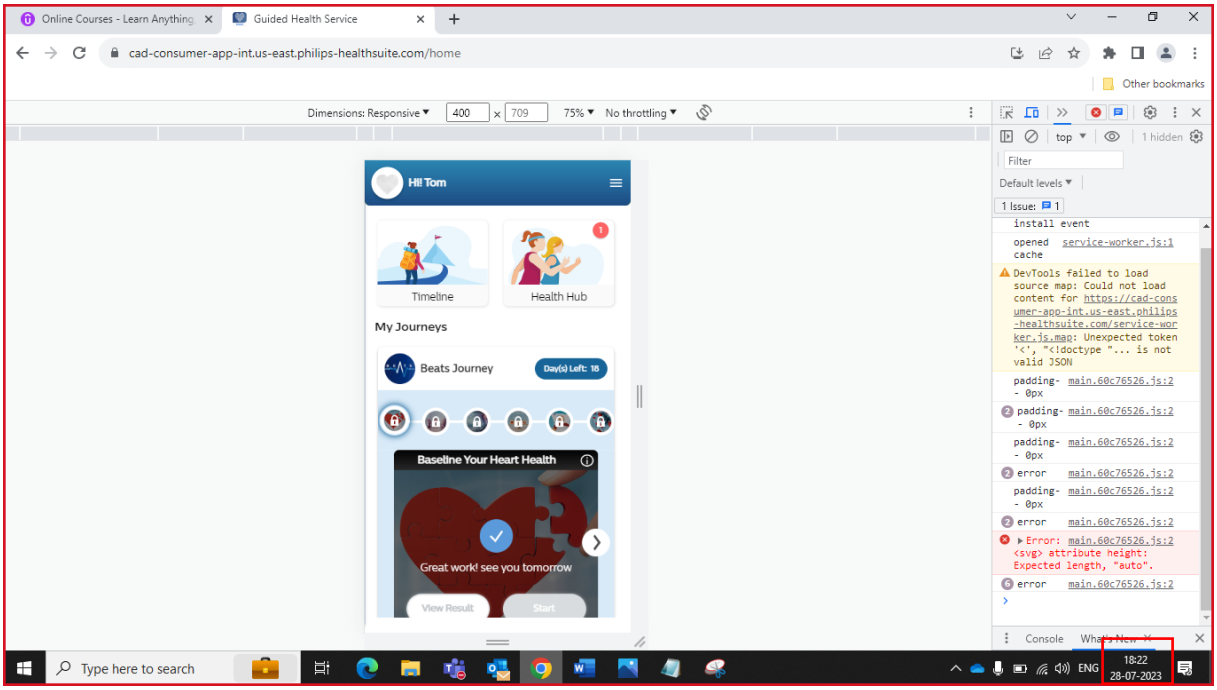
Refer the **Video POC**

Case 4:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Session time out should be shorter period of time. Session was still logged in after 60minutes.

Case 5:

Refer the **Video POC**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.8 Webapp: Lack of Authorization

Vulnerability Title	Lack of Authorization
Vulnerability Category	A1 Broken Access Control
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 6.8 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
Description	**Vulnerability Description:** The application lacks sufficient controls to prevent a user from accessing another user's functionality**.** It was observed that a non-admin user can see and modify an admin user's functionality because of lack of authorization check at server side. **Retest status (27/April/2023):** Authorization is still not implemented properly. Hence the issue is OPEN. **Retest status(2/May/2023):** Proper authorization check is in place and thereby marking this issue as 'CLOSED'. **Retest as of 24-July-2023:** The issue is Fixed. **Exploitability Rational:** The attacker needs to be an authenticated user. **Impact Rational:** Confidentiality and integrity are compromised and functionalities can be misused.
Affected Systems/IP Address/URL	https://cad-api-gateway-staging.us-east.philips-healthsuite.com/identity/Search
Recommendation	Proper authorization mechanism should be implemented on server side, validating user's access to certain resources. Explicitly check the authorization on the server-side to verify that the user making a request to view data or perform an action is authorized to do. This is simple as checking that a user is authorized to view a particular page in the application or check that the user is authorized to

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	perform an action overall. Many other more fine-grained situations may exist depending on the application context and the complexity of the business functionality. Reference: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html
Status	**Closed**

Supportive Evidence:

Refer the Video POC (non-admin user can see the resources of an admin user)

Refer the Video POC (non-admin user can see the custodian requests and after modifying the profile type from custodian to admin, able to see admin requests)

Retest status as of 27 April 2023:

Refer the Video POC (first instance is fixed)

Refer the Video POC (non-admin users can still see the custodian requests and admin requests)

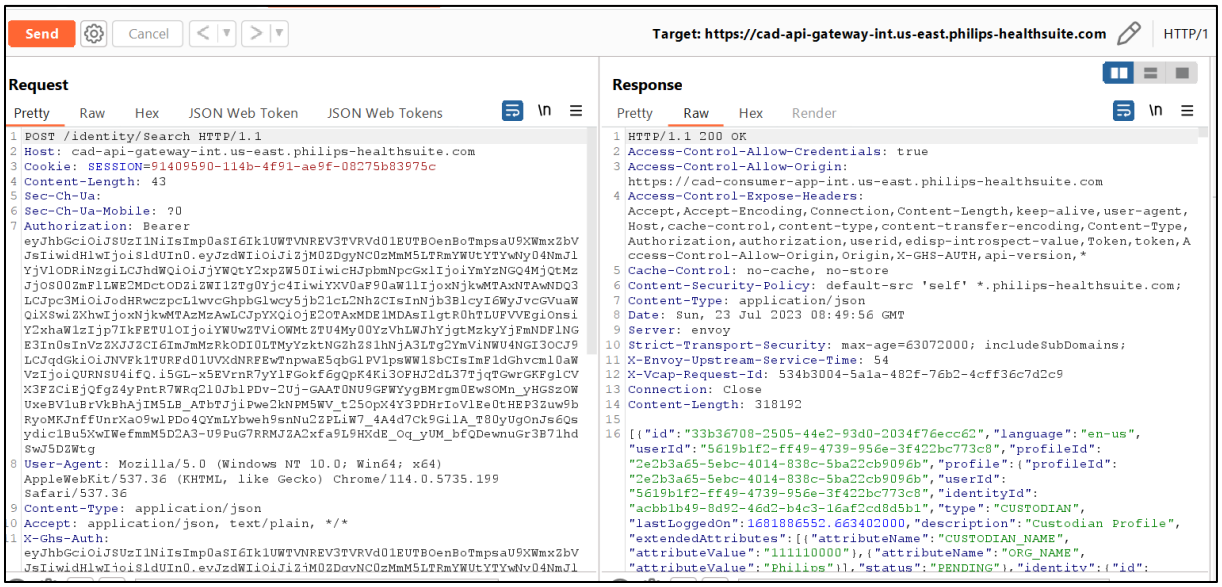
Retest status as of 2 May 2023:

Refer the Video POC

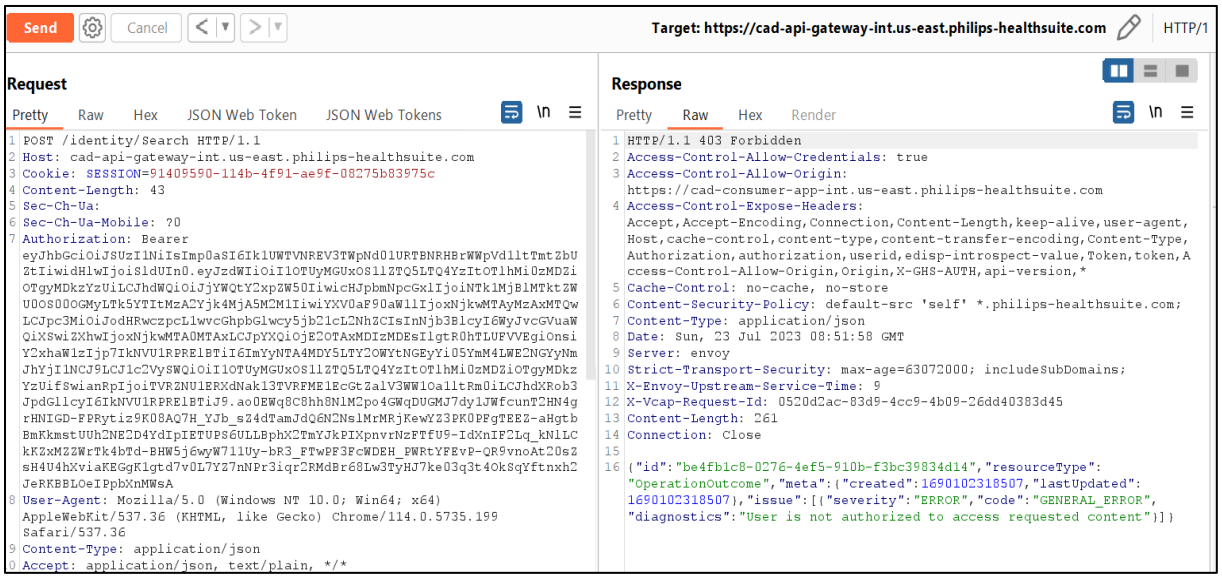
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



a. Actual request from admin user with 200ok response



b. Same Request made by Custodian User with 403 Forbidden responses

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.9 Webapp/WebServices: Sensitive Information in URL

Vulnerability Title	Sensitive Information in URL
Vulnerability Category	A2 Cryptographic Failures
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N
Description	**Vulnerability Description** Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Ideally, HTTPS URL despite encryption, are logged in plaintext in browser history, logs, trusted proxies, etc. The query string will be sent as part of the URL if the URL is passed to another site via the Referrer header. URLs sent to the user as part of an HTML page may be cached on disk. It is observed that EMAIL or Phone number and refresh token, code challenge are getting disclosed in URL. Reference: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure **Retest as of 24-July-2023:** The issue is still Valid and not fixed. **Retest as of 28-July-2023:** The issue is fixed for Case 2. For the Case 1 issue is still valid and open. **Exploitability rational** An authenticated user of the application or an attacker who should be authenticated, can access this information by crawling the application across the functionalities. The attacker can gain this information from anywhere within the network. Potential access vectors may include but are not limited to: • Browser history, proxy logs, web server logs, etc. • Shoulder-surfing the URL in a user's browser address bar.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Impact rational Exploitation of this scenario would allow attacker gather information as part of reconnaissance. Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which would allow user impersonation.
Affected Systems/IP Address/URL	https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/token?grant_type=refresh_token&refresh_token=MTY4MTI5Nzk5NTg0Mjo0ODZhZjRlNmI4OnVzZXJuYW1lPTc2NTQzMjEwOTg6MTVkMDMzY2UzMzg3MjE1Y2NhMjY4ZWUxNzFlZjEwMDFjZGFiMGIzZmQzMjgyZWZjNjE1OGYyOWIxOGYxMDgzYzAzZjc5NGVhODRjNDdkOGRlZTIyZGRjZTE0MDcyNGIyZjVhYTY3ODMzMmMzMTI5MDVlZTA2YTFjMzIxMmYzMmM=&client_id=cad-client https://cad-api-gateway-int.us-east.philips-healthsuite.com/oauth/authorize?response_type=code,token,id_token&scope=openid&client_id=cad-client&redirect_uri=https://cad-consumer-app-int.us-east.philips-healthsuite.com&login_hint=EMAIL:chaitran.shivayogimath@philips.com&code_challenge=ZVeqsAYcKTEn1D__B4yI4vrcVmSHJ9QJ6GTkdXM_eR8&code_challenge_method=SHA256 https://cad-consumer-app-int.us-east.philips-healthsuite.com/?code=97dd15307143a540818cf41950d1888ff78bc0120a4c8e9326&login_hint=cadadmin@grr.la
Recommendation	• It is recommended not to disclose internal identifiers like, variable names, system information, session information etc. • Sensitive information should be sent using POST method only. Reference: https://cheatsheetseries.owasp.org/cheatsheets/User_Privacy_Protection_Cheat_Sheet.html
Status	**Open (partially open for Case 1)**

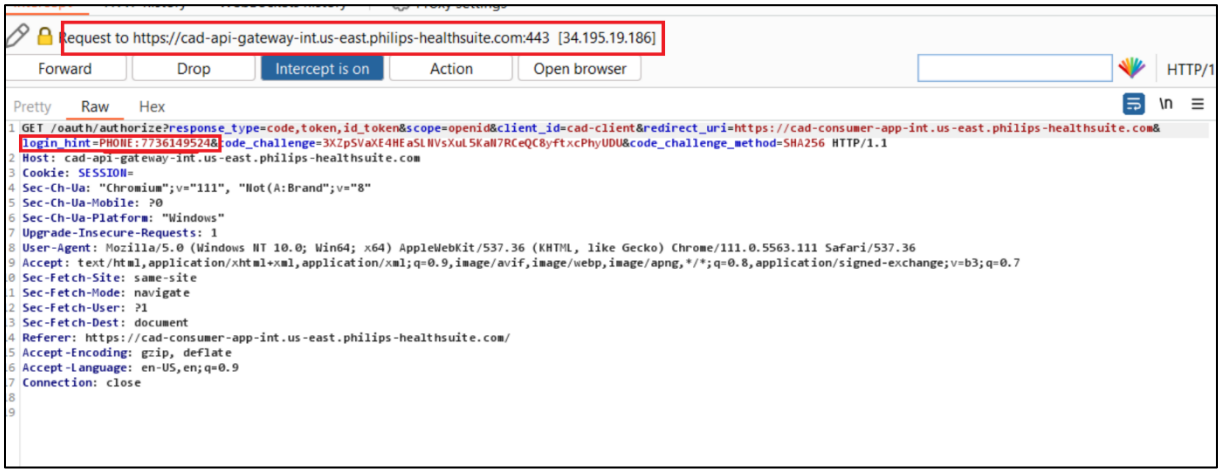
Steps to Reproduce:

Step 1: Configure the browser to use a proxy tool such as Burp Suite.
Step 2: Intercept the request and observe that the sensitive information has been passed in the URL as shown in the below screenshot:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Refresh token getting disclosed in URL



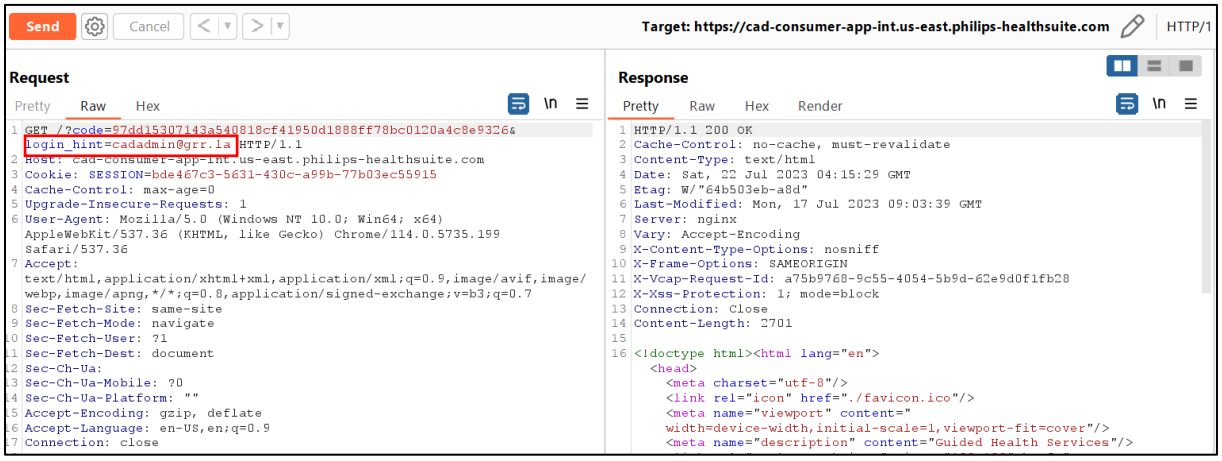
Phone number getting disclosed in URL

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Case 1:

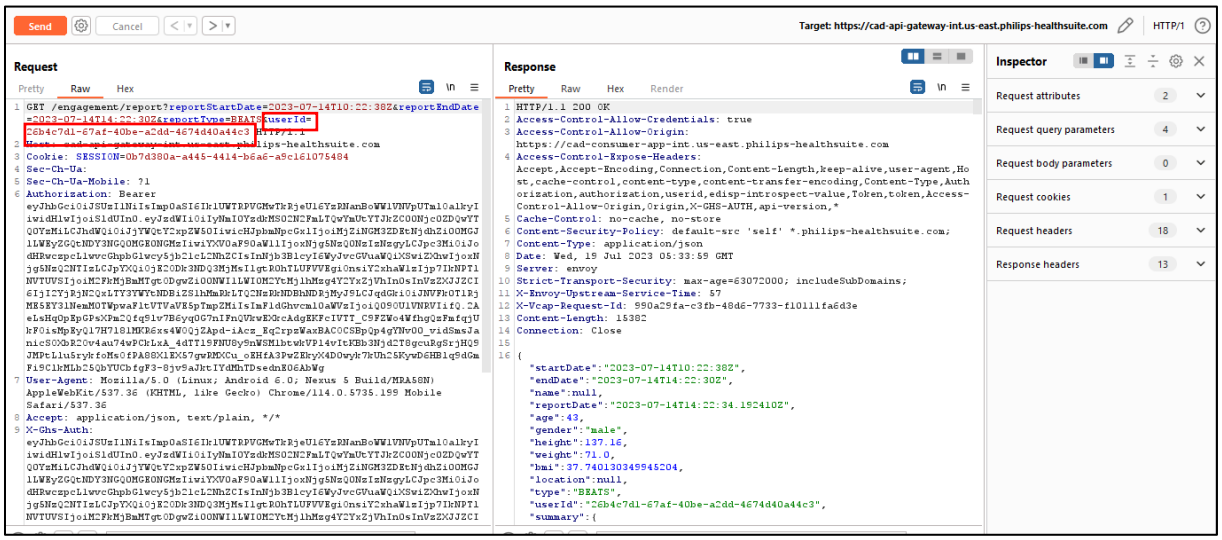
Retest Status as of 24th July 2023



Email ID is visible under url

Case 2:

Test Evidence as of on 24 July 2023:

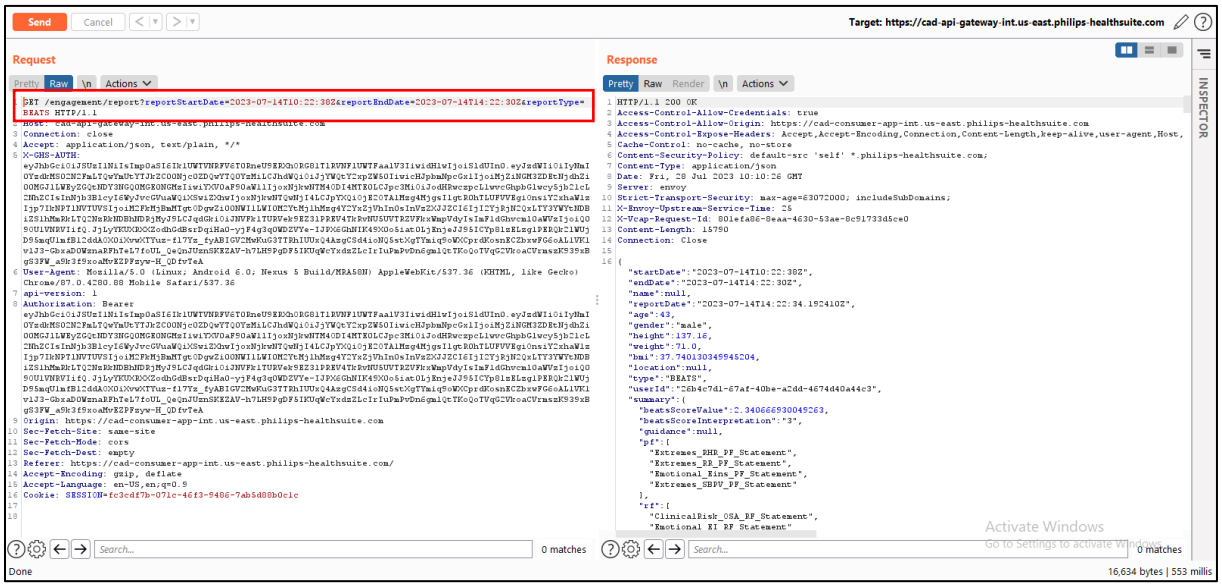


Sensitive information disclosed

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Evidence as of on 28 July 2023:



Sensitive information is not visible and fixed in next build

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.10 Webapp: Misconfigured CORS

Vulnerability Title	Misconfigured CORS
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
Description	**Vulnerability Description:** During security assessment it is observed that the server is configured with an unrestricted HTML5 Cross-Origin Resource Sharing (CORS) policy. CORS defines whether resources on other domains can interact with this server. An attacker can place malicious JavaScript on his domain that can exploit the unrestrictive CORS policy to access sensitive data on this server or perform sensitive operations without the user's knowledge. Additionally, an attacker could exploit security vulnerabilities on other domains to compromise services on this server. The CORS policy relaxes the Same Origin Policy, an important security control that isolates potentially malicious resources to its respective domain name. If a script attempts to violate the Same Origin Policy by interacting with another domain, modern browsers can check a server's CORS policy by issuing a "pre-flight request". The browser allows the interaction only if the server responds with an Access-Control-Allow-Origin header that lists the script's domain or a wildcard match (*). A wildcard match allows interaction from any other domain, which allows any malicious content to retrieve content from this server or perform user actions. **Retest status(17/April/2023):** It is observed that CORS Misconfiguration is still not rectified. Hence the issue is OPEN. **Retest status (26/April/2023)**: It is observed that CORS Misconfiguration has been rectified. Hence marking this issue as CLOSED. **Retest status (24/July/2023)**: Issue has been fixed.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

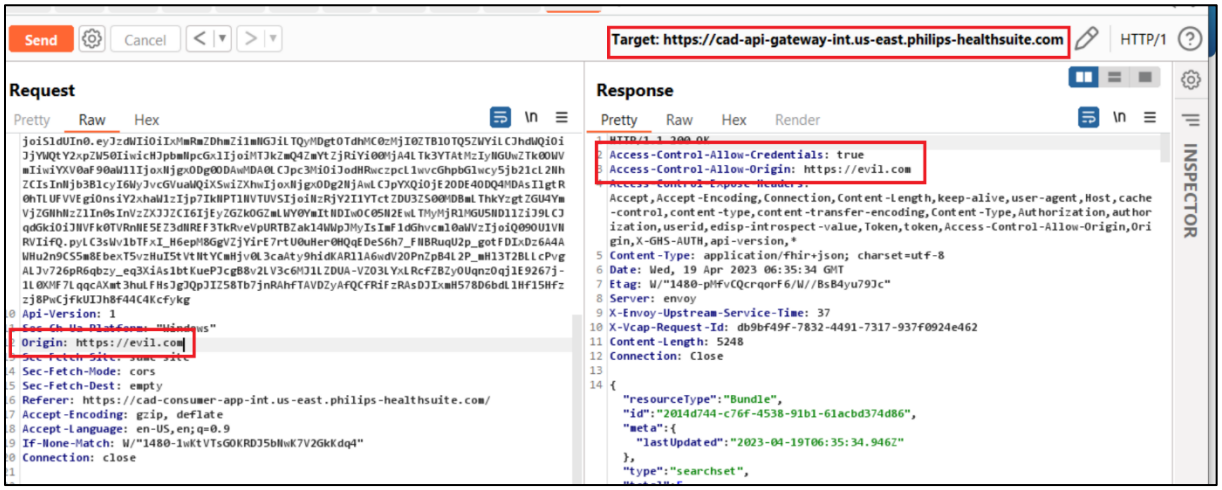
	Exploitability Rational: An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. Malicious JavaScript can perform these actions even if the server uses Cross Site Request Forgery tokens. **Impact Rational:** An attacker can access sensitive data of victim. An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007)
Affected Systems/IP Address/URL	https://cad-api-gateway-staging.us-east.philips-healthsuite.com/phr?subject=bbaa6ab0-9832-4b31-bb23-9d5fad8b90cc&_sort=-effectiveDateTime&_count=1&category=ehi *Note: This is an issue with entire application endpoints. Instances are not limited to the above items. Fix should be applied across the collection.*
Recommendation	The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. If the application requires a relaxation of the Same Origin Policy, the AccessControl-Allow-Origin header should whitelist only domains that are trusted by this server. Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
Status	**Closed**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Supportive Evidence:

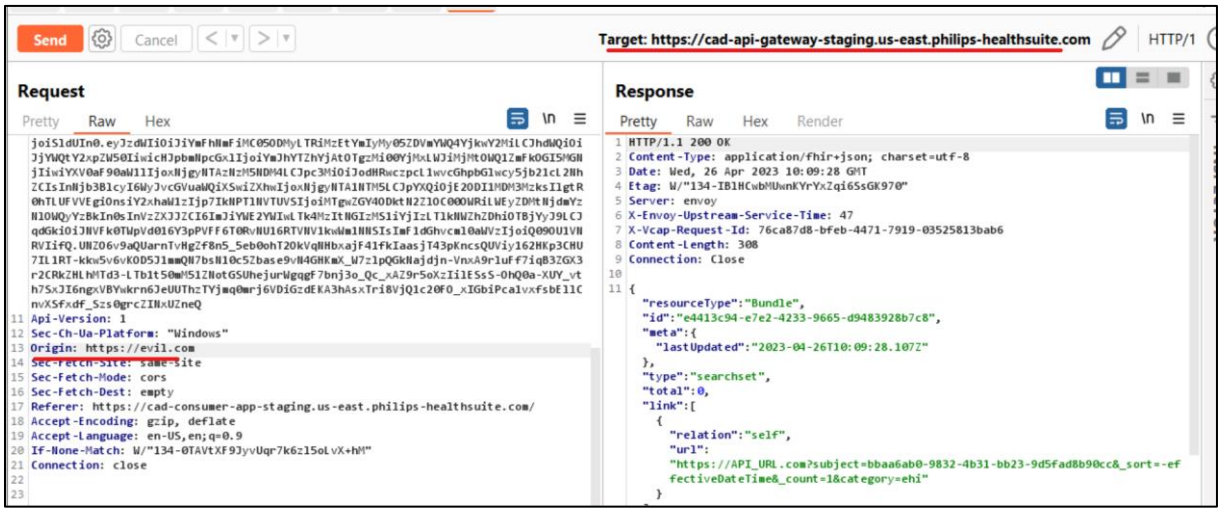
Retest status as of 17 April,2023:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest status as of 26 April, 2023:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.11 Webapp/WebServices: HTTPS Fallback Allowed

Vulnerability Title	HTTPS Fallback Allowed
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the assessment, it was observed that the below mentioned endpoints supported HTTP as well. By default, API's are served in HTTPS, but the connection can be downgraded to HTTP. **Retest status(17/April/2023):** It was observed that the issue persists for some domains. **Retest as of 24-July-2023:** The issue is still Valid and not fixed. **Exploitability Rational:** If a victim accesses the application with an HTTP-based URL, an attacker listening on any network between the victim and the application server may view and modify application traffic. **Impact Rational:** Attacker can perform Man in the middle attack also can see all communication in clear text
Affected Systems/IP Address/URL	http://cad-consumer-app-int.us-east.philips-healthsuite.com/ https://cad-cardiovital-app-int.us-east.philips-healthsuite.com/ WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report
Recommendation	• HTTPS should be enabled and enforced on the application server. Once HTTPS has been properly configured, ensure that the application requires HTTPS for access to all application resources, including JavaScript files, style sheets, and images. When a user attempts to navigate to any part of the application over HTTP, the application should redirect the user to the HTTPS version of the application.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

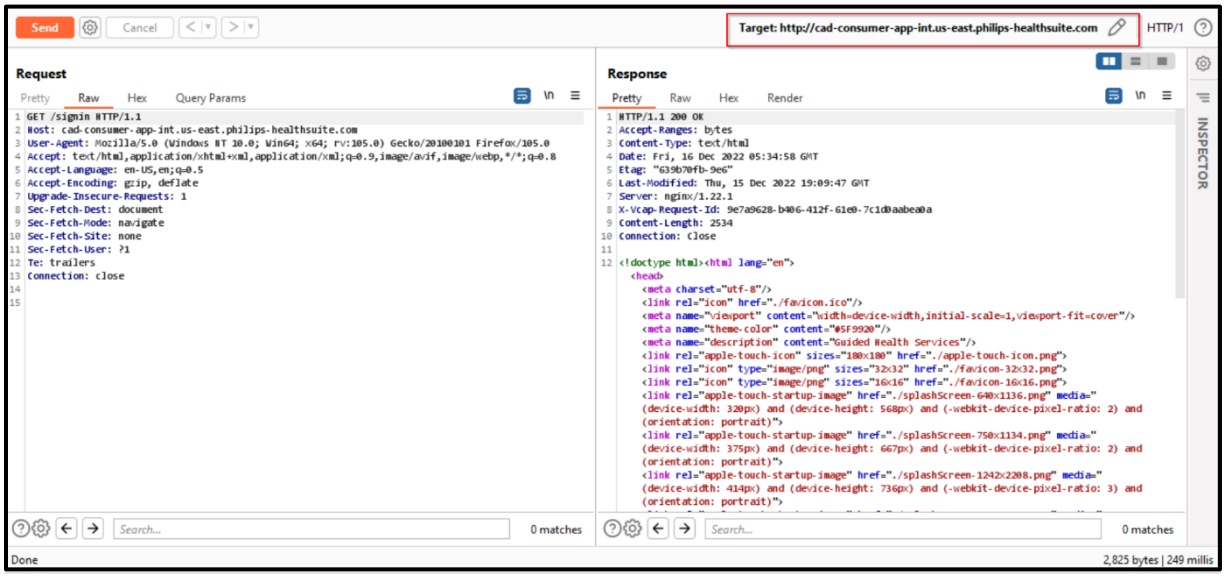
Printed copies are uncontrolled unless authenticated.

	• it is recommended that applications are deployed with **HTTP Strict Transport Security (HSTS)**. HSTS forces the browser to access a site only over HTTPS and prevents access in cases where the authenticity of the X.509 certificate cannot be verified. HSTS is supported in recent versions of the Chrome, Firefox, and Opera web browsers. To enable HSTS, simply add the Strict-Transport-Security header to the response header when users first access the site over HTTPS. References: • https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html • https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
Status	**Open**

Steps to Reproduce

Step1: Capture the application request in Burp, which is running on port 443.

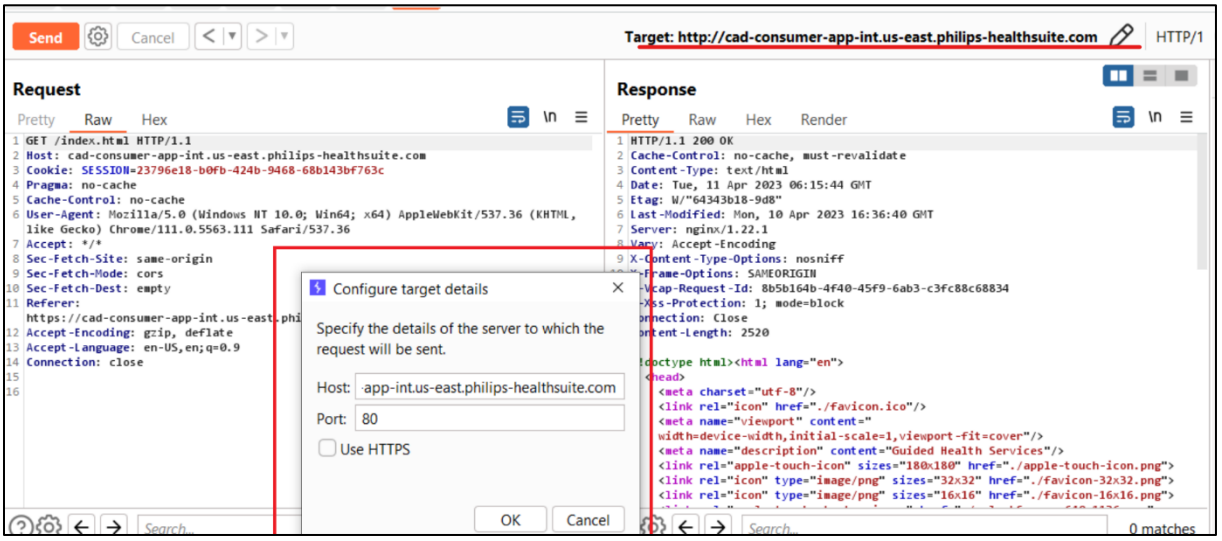
Step2: Now click on the target bar and uncheck the https, upon sending the request with port 80, a proper response captured as shown below screenshots.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

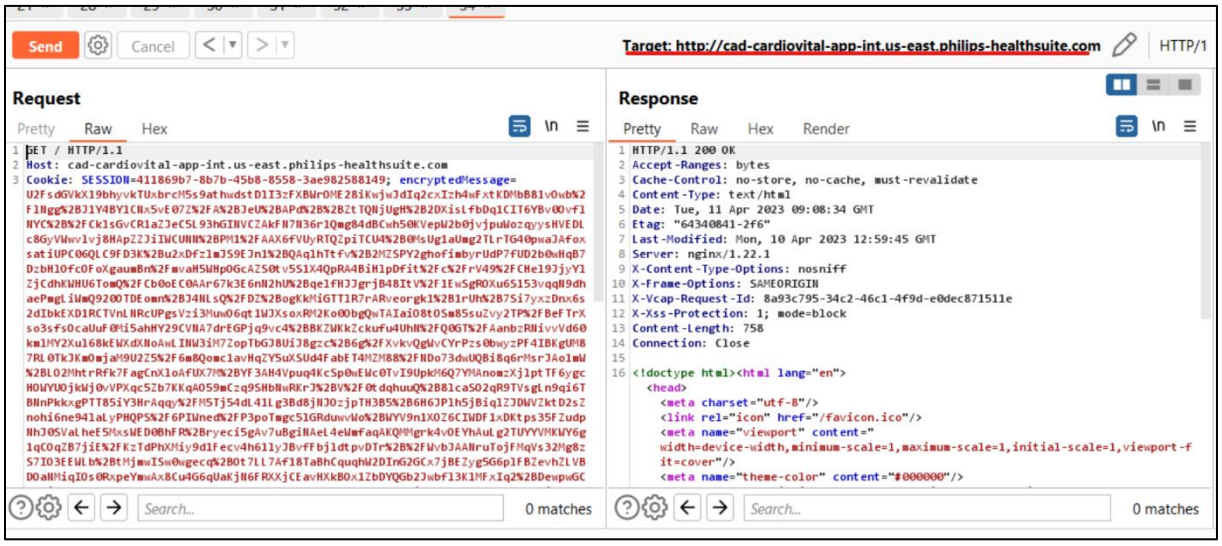
Printed copies are uncontrolled unless authenticated.

Retest status as of 17/April/2023:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023:

Case 1: WebApp

Allowed HTTPS Fallback

Case 2: WebServices

Refer the **Video POC**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.12 Webapp/WebServices: Server Banner Disclosure

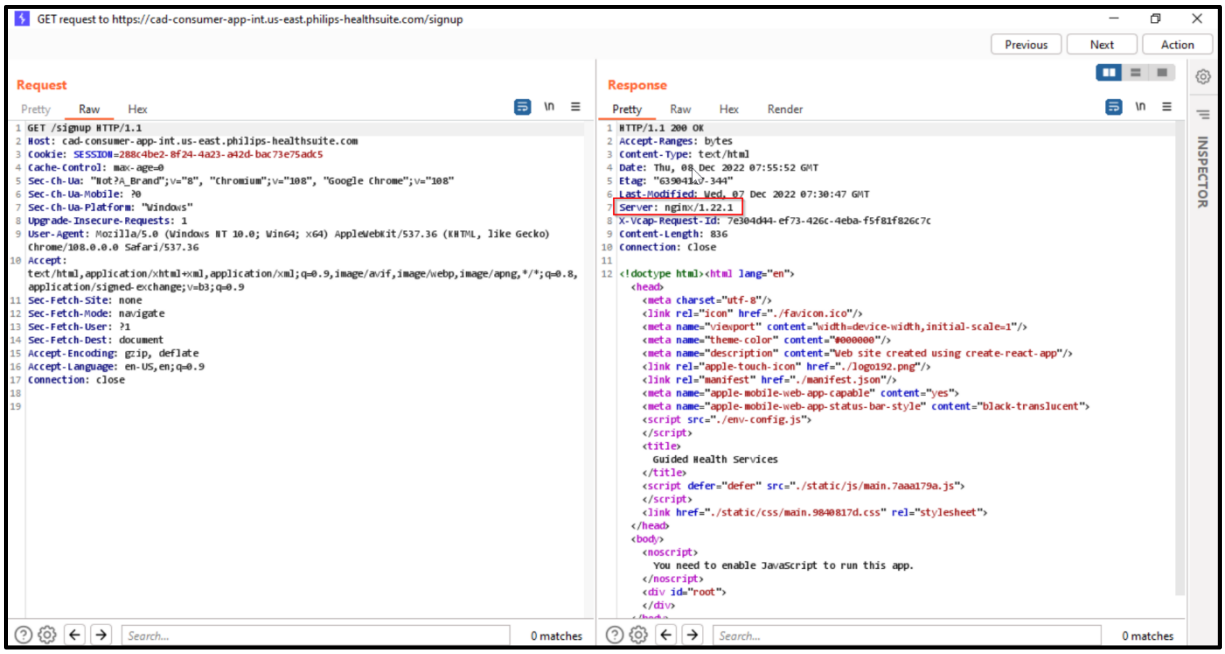
Vulnerability Title	Server Banner Disclosure
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the security assessment, it was found that the application discloses the application server details including the version in the HTTP response. Targeted attacks can be launched against the server based on the exploits it is having. It was observed that the server nginx 1.22.1 is being used. **Retest (17/April/2023):** Server information is still getting disclosed. It was observed that nginx 1.24.0 and envoy are used. Nginx 1.24.0 has a known vulnerability "Access Restriction Bypass". Refer: https://snyk.io/test/docker/nginx%3Astable **Retest as of 24-July-2023:** The issue is Fixed. **Exploitability Rational:** Web server fingerprinting is a critical task for the penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing and those are available on internet. **Impact Rational:** Targeted attacks can be launched against the server based on the exploits it is having.
Affected Systems/IP Address/URL	WebApp: https://cad-cardiovital-app-int.us-east.philips-healthsuite.com https://cad-consumer-app-int.us-east.philips-healthsuite.com https://cad-api-gateway-int.us-east.philips-healthsuite.com WebService Endpoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Recommendation	It is recommended to use custom banner for server by hiding all sensitive information from banner.
Status	**Closed**

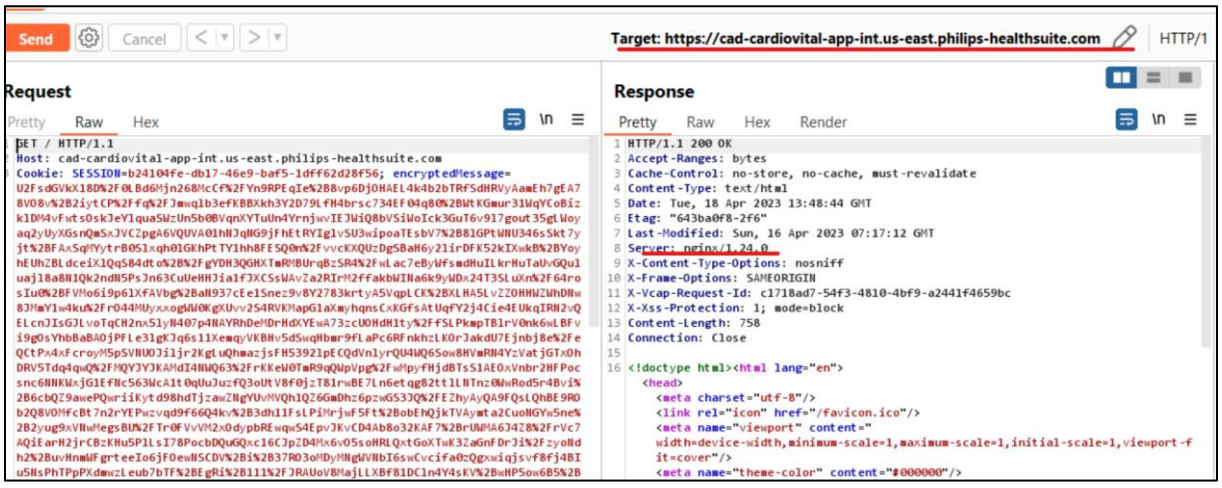
Steps to Reproduce



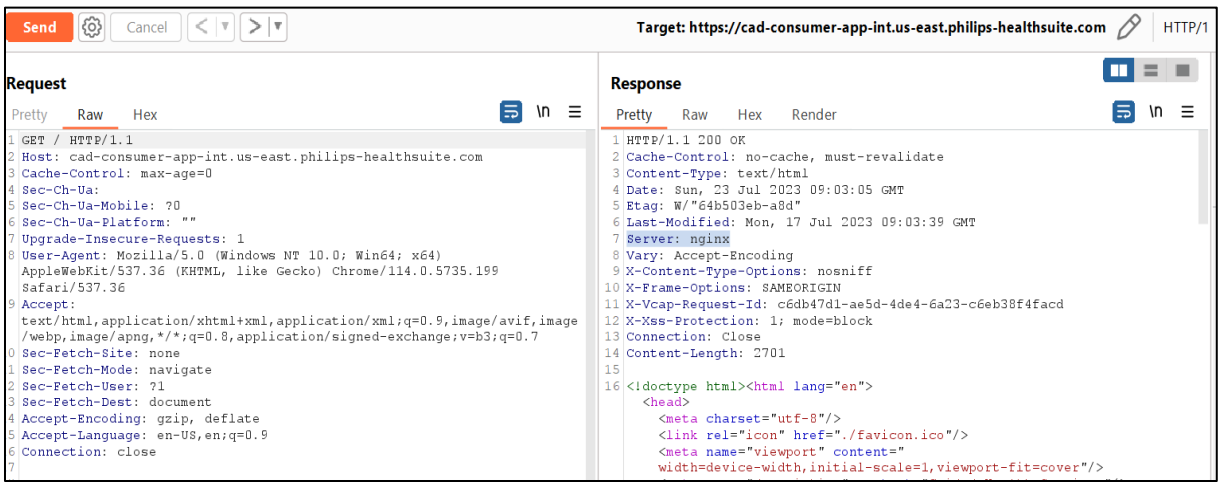
Retest (17/April/2023):

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

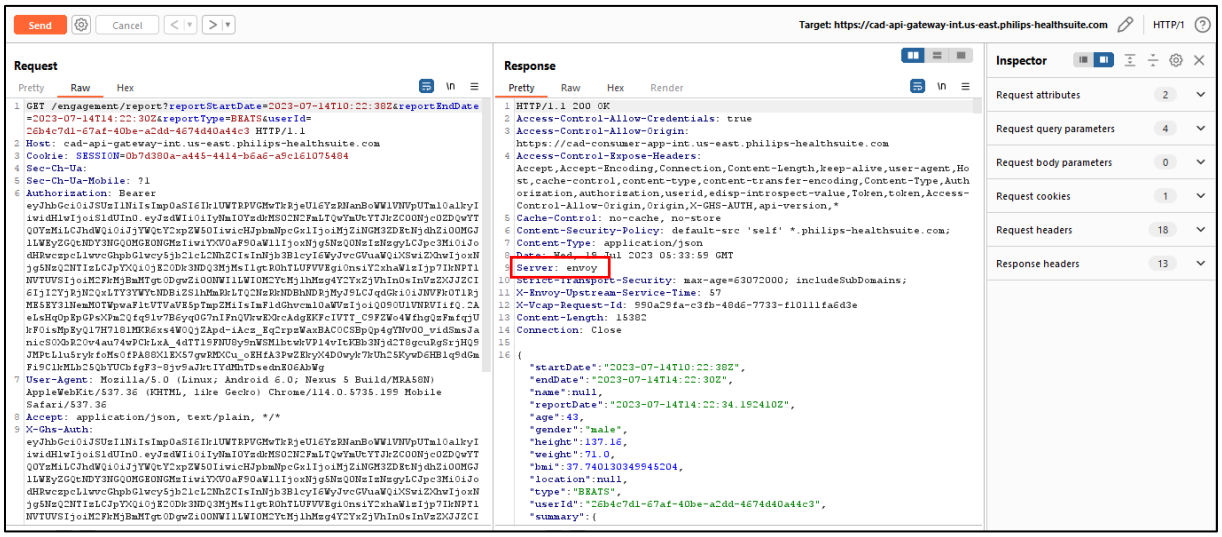


Retest Status as of 24th July 2023



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.13 Webapp/WebServices: Improper Error Handling

Vulnerability Title	Improper Error Handling
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description** Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden. Reference: https://owasp.org/www-community/Improper_Error_Handling **Retest as of 24-July-2023:** The issue is still Valid and not fixed. **Exploitability rational** An attacker should have access to the application. **Impact rational** By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.
Affected Systems/IP Address/URL	WebApp: https://cad-api-gateway-int.us-east.philips-healthsuite.com WebService EndPoint: https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report
Recommendation	The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

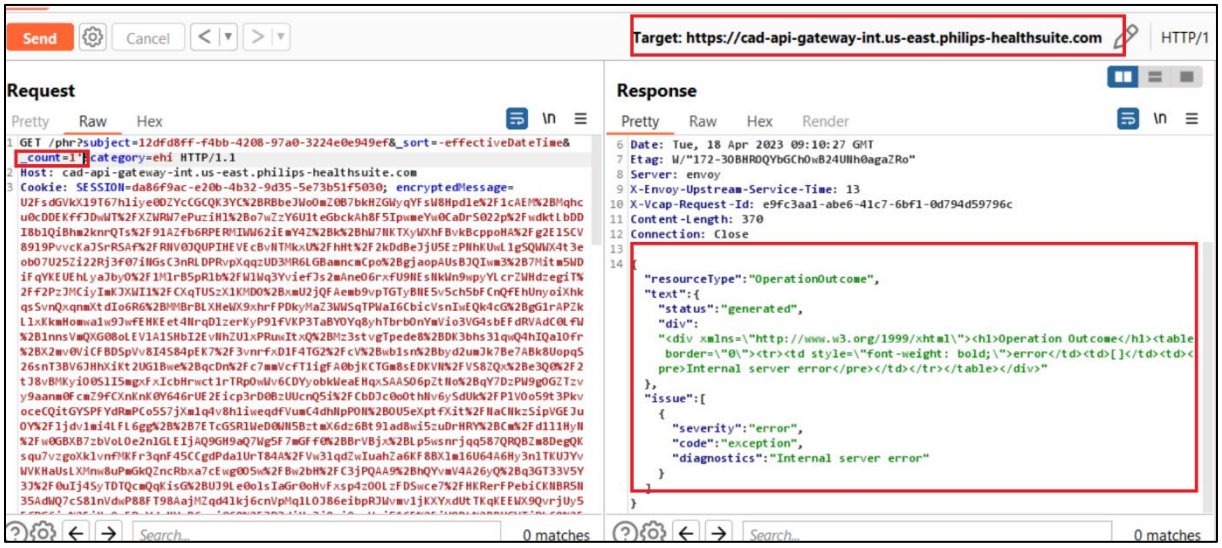
	References: • https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html • Improper-Error-Handling-Fix-In-JAVA • Improper-Error-Handling-Fix-In-ASP.NET-Core • Improper-Error-Handling-Fix-In-SpringBoot
Status	**Open**

Steps to Reproduce:

Step 1: Configure the browser to use proxy tool such as Burp Suite.
Step 2: Capture a request containing some input fields and send it to the Repeater tool.
Step 3: Manipulate the request with certain malicious characters in the input fields and observe that there is error disclosure in the response as shown in the screenshot below:

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

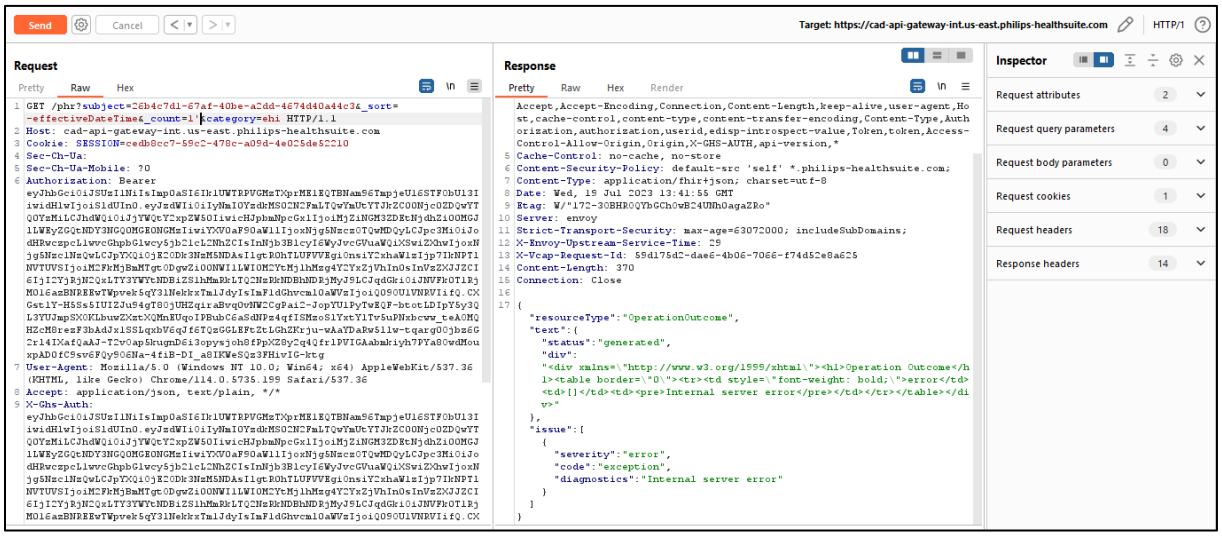


On adding single quote, internal server error is shown with a detailed error message

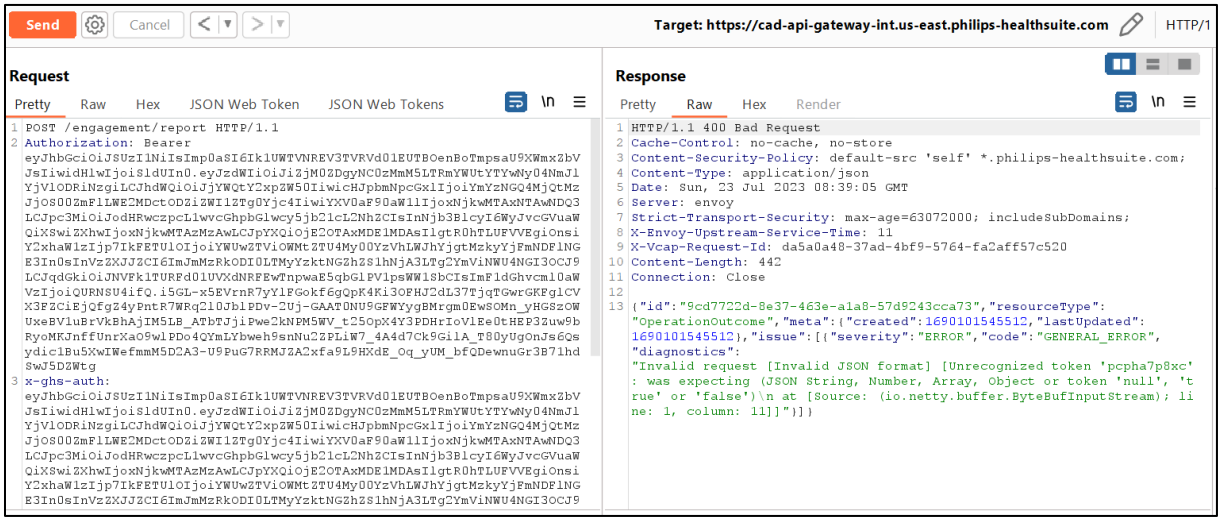
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Retest Status as of 24th July 2023



Improper error handelling



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.14 Webapp: Missing Security Headers

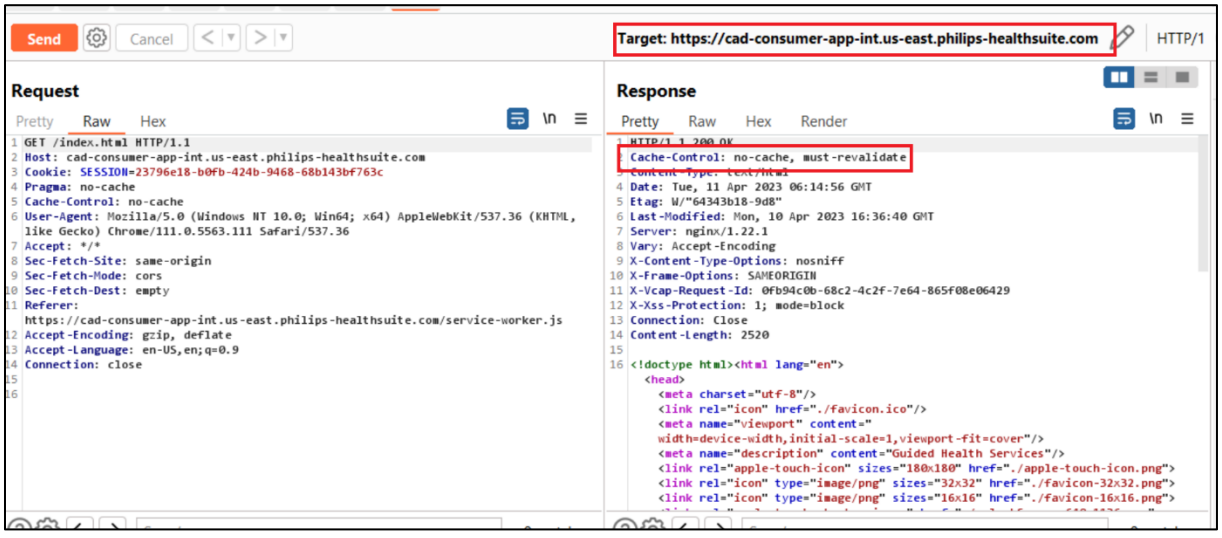
Vulnerability Title	Missing Security Headers
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.9 CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L
Description	**Vulnerability Description:** During security assessment, we found that either the security headers are not configured properly, or security headers are missing in response. Security headers in the response can be used to increase the security of the application. The missing security headers are: • Content-Security-Policy: default-src 'self' xyz.abc.company.com; • Cache-Control: no cache, no store • Strict-Transport-Security: max-age=31536000; includeSubDomains; Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers **Retest as of 24-July-2023:** The issue is still Valid and not fixed, CSP not implemented. **Exploitability rational** Exploitability of these depends differently based on the missing headers. Like Cache-Control headers require physical access to the system. But others require user interaction to exploit this vulnerability.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Impact rational These headers provide the additional security at client side. Missing these headers may lead to sensitive information disclosure like account take over etc.
Affected Systems/IP Address/URL	https:// cad-api-gateway-int.us-east.philips-healthsuite.com https://cad-consumer-app-int.us-east.philips-healthsuite.com
Recommendation	It is recommended to configure all the security headers in the response to improve your application's security. References are provided in the below links: • https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html • https://owasp.org/www-project-secure-headers/ • https://help.deepsecurity.trendmicro.com/20_0/on-premise/http-security-headers.html
Status	**Open**

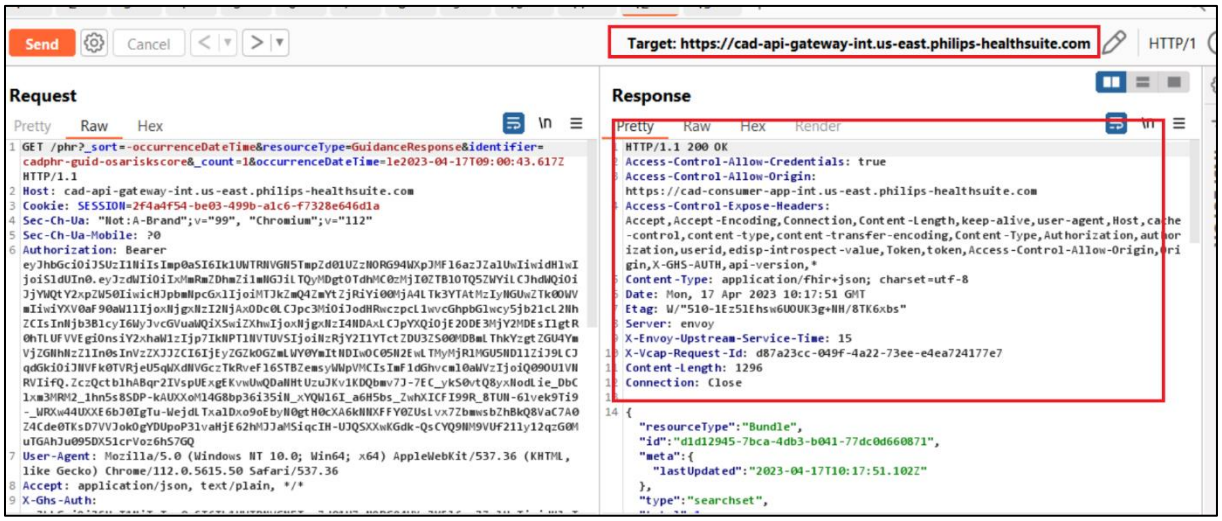
Supportive Evidence:



no-store directive not set, CSP not set, HSTS not set

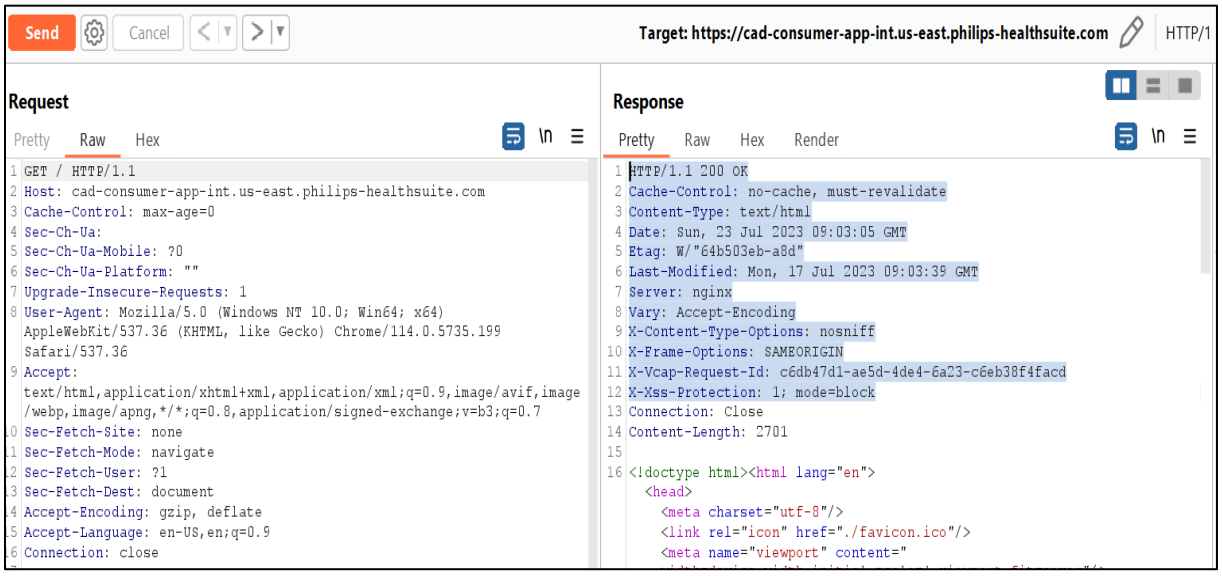
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Cache control, CSP, HSTS not set

Retest Status as of 24th July 2023



no-store directive not set, CSP not set, HSTS not set

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.15 Webapp: Sensitive file exposed

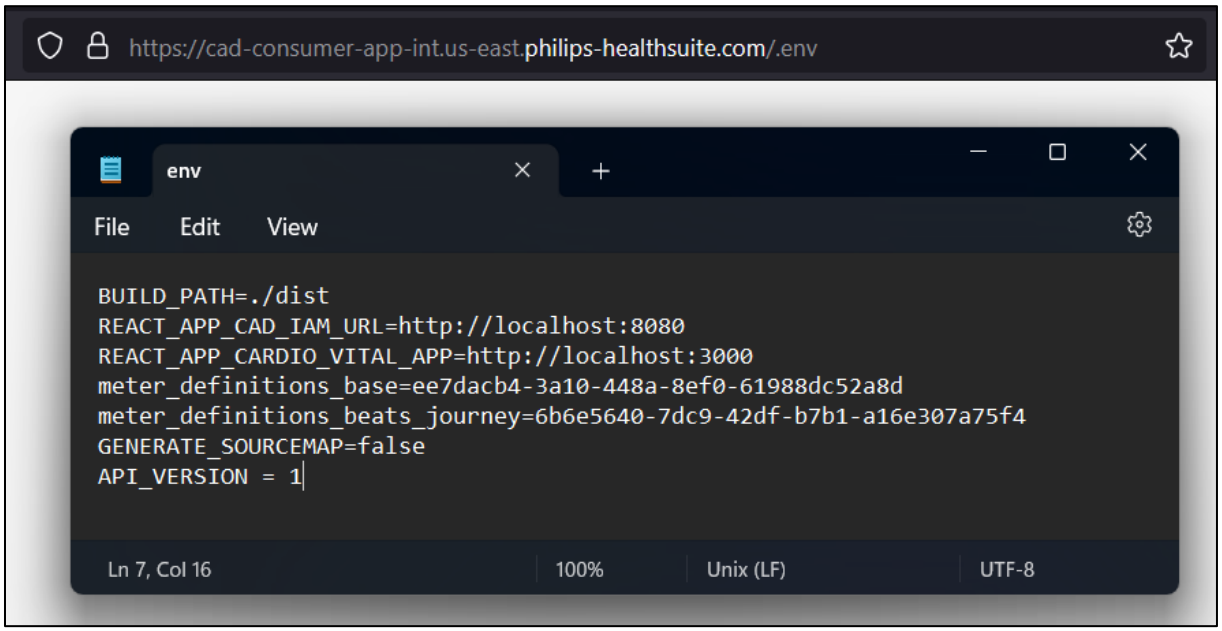
Vulnerability Title	Sensitive file exposed
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. **Test as of on 24 July 2023:** Identified sensitive file. Issue is open. **Exploitability rational** To Exploit this vulnerability, attacker just need access to this webapplication and run directory bruteforce on top of the domain endpoint. **Impact rational** These kind fo configuration file helps attacker to make more sophisticated attacks.
Affected Systems/IP Address/URL	https://cad-consumer-app-int.us-east.philips-healthsuite.com/.env
Recommendation	Restrict access to this file or remove it from the website.
Status	**Open**

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Supportive Evidence:

Test Evidence as of on 24 July 2023:



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.16 Webapp: User Email Enumeration

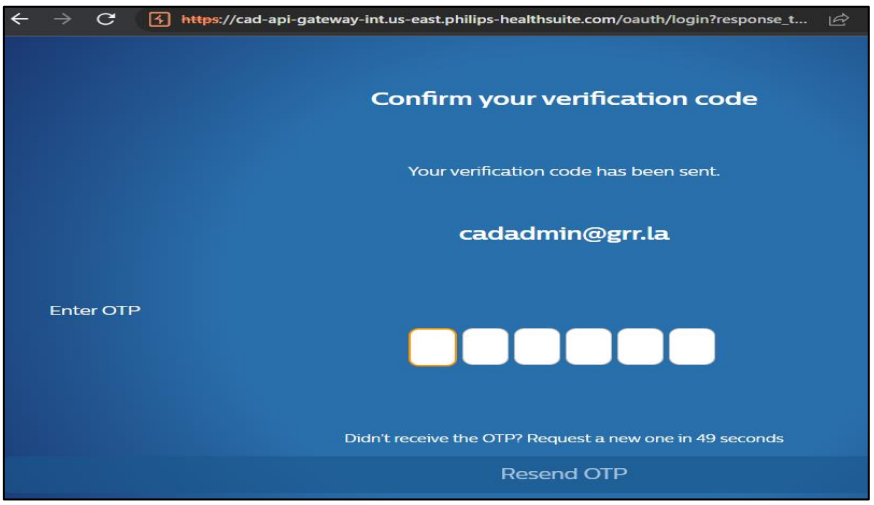
Vulnerability Title	User Email Enumeration
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** It was observed that the application sigin endpoint returned verbose error messages upon authentication, indicating whether the supplied email address exists in the application. **Test as of on 24 July 2023:** **Case 1:** User Email is visible after sending the OTP. **Case 2:** Unregistered email mentioned in error message. **Exploitability rational** An attacker must be aware of or identify the pattern of email address in use to automate attacks against the authentication mechanism. Even when a email address could be identified by an attacker, it is reasonably difficult to guess the coressponding passwords using bruteforce techniques. Thus it appears highly unlikely to be exploited. **Impact rational** User email enumeration vulnerabilities may be abused by malicious users to identify valid email address of the application. These can be leveraged for further attacks such as password bruteforcing. Furthermore, attackers can use identified valid email address to perform Denial of Service attacks by locking out these accounts.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://cad-consumer-app-int.us-east.philips-healthsuite.com/signin
Recommendation	It is recommended to Implement the authentication mechanism such that the application displays generic error messages such as " OTP will be sent to your registered email ID". Furthermore the application should not provide other indicators in the response such as different error codes.
Status	**Open**

Supportive Evidence:
Case 1:

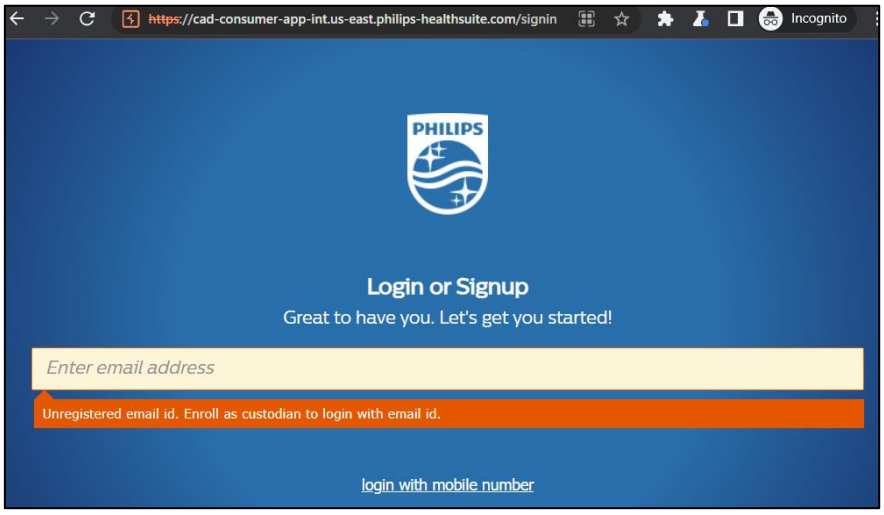


a. Above screenshot shows the response for valid email address

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Case 2:



b. Above screenshot shows the response for invalid email address with verbose error message "Unregistered email ID"

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

7.17 WebServices: Misconfigured CORS

Vulnerability Title	Misconfigured CORS
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
Description	**Vulnerability Description:** During security assessment it is observed that the server is configured with an unrestricted HTML5 Cross-Origin Resource Sharing (CORS) policy. CORS defines whether resources on other domains can interact with this server. An attacker can place malicious JavaScript on his domain that can exploit the unrestrictive CORS policy to access sensitive data on this server or perform sensitive operations without the user's knowledge. Additionally, an attacker could exploit security vulnerabilities on other domains to compromise services on this server. The CORS policy relaxes the Same Origin Policy, an important security control that isolates potentially malicious resources to its respective domain name. If a script attempts to violate the Same Origin Policy by interacting with another domain, modern browsers can check a server's CORS policy by issuing a "pre-flight request". The browser allows the interaction only if the server responds with an Access-Control-Allow-Origin header that lists the script's domain or a wildcard match (*). A wildcard match allows interaction from any other domain, which allows any malicious content to retrieve content from this server or perform user actions. **Test as of on 24 July 2023:** Identified Misconfigured CORS. Issue is open. **Retest as of on 28 July 2023:** Issue is fixed. **Exploitability Rational:** An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. Malicious JavaScript can perform these actions even if the server uses Cross Site Request Forgery tokens.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

	Impact Rational: An attacker can access sensitive data of victim. An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge. https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007)
Affected Systems/IP Address/URL	https://cad-consumer-app-int.us-east.philips-healthsuite.com/engagement/report *Note: This is an issue with entire application endpoints. Instances are not limited to the above items. Fix should be applied across the collection.*
Recommendation	The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. If the application requires a relaxation of the Same Origin Policy, the AccessControl-Allow-Origin header should whitelist only domains that are trusted by this server. Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
Status	**Closed**

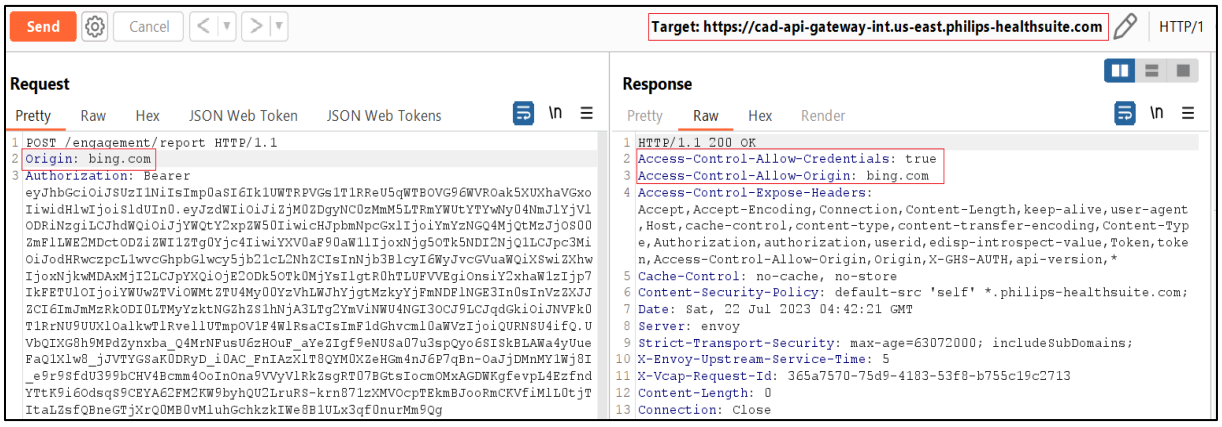
Supportive Evidence:

Test Evidence as of on 24 July 2023:

Identified Misconfigured CORS (GET)

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



Identified Misconfigured CORS (POST)

Retest Evidence as of on 28 July 2023:

Same origin is configured. Issue is fixed

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

8. Tools Used

Scope	Tools Used
Web Application/Web Services Security	BurpSuite Pro, NMAP, Postman

9. Automated Tool Report

sslscan.txt

10. Manual Test Reports and Test Case Execution

2695_CAD_GHS_SCo
E_Security_Assessmer

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.